NASA Contractor Report 3534

A System Safety Model for Developmental Aircraft Programs

Emil J. Amberboy and Robert L. Stokeld

CONTRACT NAS2-10361
APRIL 1982

NASA

NASA Contractor Report 3534

A System Safety Model for Developmental Aircraft Programs

Emil J. Amberboy and Robert L. Stokeld
Boeing Aerospace Company
Houston, Texas

Prepared for
Ames Research Center
under Contract NAS2-10361

National Aeronautics
and Space Administration

Scientific and Technical
Information Branch

1982

CONTENTS

Section | Page

FIGURES

Section		Page

EXECUTIVE SUMMARY

This document presents some basic tenets of safety as applied to developmental aircraft programs. It does not discuss the philosophy of system safety nor does it present instructions for applying system safety principles to a project. Rather, the integration of safety into the project management aspects of planning, organizing, directing, and controlling is illustrated by examples. The examples presented here are taken from the joint NASA/Army Rotor System Research Aircraft (RSRA) project which has maintained an enviable safety record through several years of development and operation.

The RSRA project was initiated in 1973 to produce vehicles for conducting advanced rotor systems research. The project resulted in production of two highly instrumented aircraft capable of flying in the fixed-wing, helicopter or compound modes. The specifications established a performance envelope that exceeded normal helicopter performance in many ways while stressing adaptability to new rotor systems, precisely controlled test conditions, and measurement accuracy. Fulfillment of these specifications required advancement of state-of-the-art technology in many areas, such as provision for crew escape in an emergency. It also required close coordination between NASA and contractor personnel. This, in turn, necessitated formulation of unusual communication protocols which fostered development of a "project family" attitude.

The RSRA project office was originally based at Langley Research Center and operated within the confines of a typically austere research and development budget. During later stages of development the project was transferred to the Ames Research Center resulting in general loss of corporate memory and necessitating changes in the system safety program to compensate for this loss.

To begin an overview of the RSRA safety program, it would be well to understand the attitude and philosophy of the former RSRA Project Manager/Chief Engineer, Sam White, Jr. His approach to safety on the project was guided by the following philosophy:

"The system safety program that evolved on the RSRA was based on a set of concepts, some basic system safety principles, and on a fairly limited set of guidance documents. A list of some pretty basic (yet very useful) principles was used in developing the RSRA system safety program (courtesy of Chuck Miller's George Washington University program on aviation safety):

a. Accidents are unplanned, but controllable combinations of events.

b. Accidents are rare; hazards (risks) are not.

c. Combinations of "acceptable" hazards produce accidents.

d. Accidents are usually caused by a sequence of complex cause-effect relationships that may be obscured by simplistic probable/proximate cause determinations.

e. Cause-prevention determination should include factors of:

- Man (human error, workload).
- Machine (failure, design defect).
- Medium (environment).
- Management (attitude, motivation, control).
- Mission (nature, urgency).
- Money (cost/safety tradeoffs).

f. Safety is an integral part of mission accomplishment (economic, survival).

g. Accident prevention is more than accident investigation and cause-corrective action determination.

h. Managers/supervisors can delegate/assign safety authority/actions but cannot delegate accountability.

i. A data bank of known precedents exists for risks and corrective actions.

j. Hazard/accident reporting must emphasize corrective action, including rule enforcement, without seeking to punish improper action.

k. Human hyperawareness of high risk often results in a higher level of safety.

l. Safety tasks are finite, identifiable, definable, and do-able. Competently done, they reduce accidents.

- Define requirements (process and results, not procedures: What, not how).
- Prepare plans (road map, who/what/when).
- Conduct hazard analyses.
- Develop emergency as well as normal procedures.
- Conduct program reviews (use jury approach).
- Influence behavior (educate, train, indoctrinate, motivate, correct).
- Conduct surveys, audits, inspections.
- Use known precedent centers.
- Investigate accidents/incidents (determine cause, take corrective action, follow-up).
- Provide staff "Chaplain," ombudsman (opens free communication, emphasizes correction, deemphasizes punishment, provides liaison).

The list of safety tasks under the last bullet is particularly useful in planning a system safety program."

The applications of these and the other basic principles are illustrated in detail throughout the text.

The methods by which safety would be achieved were documented in an Airworthiness Qualification Plan (AQP) developed early in the project. The requirements specified by the AQP were carefully tailored to fit the specific RSRA mission objectives and to satisfy the intent of agency criteria.

The RSRA project budget did not permit a large safety cadre. Therefore, a safety focal point was established and the entire project staff became involved in the attainment of safety objectives. Safety goals became project goals and increased safety consciousness of the staff resulted. Resource allocations were altered when necessary to provide for performance of safety tasks of most benefit. This "horse-trading" of resources involved some risk which project management accepted when necessary, but as a conscious act, not through ignorance or default. This bold stance was justified because management remained deeply involved in safety activities throughout project development.

In the final synopsis of RSRA safety experience, it should be noted that safety goals were given in terms of positive actions. That is, negative connotations were avoided with reference to safety, and attitudes were fostered to keep safety in concert with other project activities.

It was recognized early in the project that even ultra-attention to safety in the design and ground test phases would not assure operational safety without in-depth knowledge and awareness by the flight team. For this reason, both Government and contractor flightcrews were involved throughout the design, development, test and evaluation (DDT&E) process.

While the RSRA experience was not a perfect example of "doing everything right," it came close. Some painful lessons were learned, especially relative to safety impacts of schedule slippages, transfers of roles and missions, and associated loss of corporate memory. However, flexibility was found to be a key. When events beyond project management control led to schedule impacts, slippage was allowed, but not loss of project control.

In the words of the RSRA Chief Engineer, "The fact that the project matured effectively and without incident is believed to be a <u>direct</u> result of the breadth and depth of safety planning and the in-depth involvement of all hands in safety plan implementation. The point is that the energies devoted to safety tasks are not all <u>penalties</u> to be suffered out of the need for safety; they produce <u>benefits</u> that enhance operational efficiencies, safety aside."

1.0 INTRODUCTION. This document explores those aspects of project activities required to facilitate development and implementation of a safety plan and practices which fit aircraft development or modification projects. Properly tailored, safety tasks are finite, identifiable, definable, and do-able. Competently done, they reduce accidents and make significant cost and performance effective contributions to the project.

The guidance provided in this document for tailoring a safety program uses the experience gained from the NASA/Army Rotor Systems Research Aircraft (RSRA) project. The RSRA project planning, organizing, directing, and controlling activities enabled the identification of safety requirements and tools and implementation of a plan which met the unique needs of the project.

The RSRA experience was selected as a model for a number of reasons: Safety was an integral part of the project; the project was current (development and start of operation spanned the middle 1970's to early 1980); both evolutionary and revolutionary state-of-the-art techniques were used; an austere, cost-conscious environment prevailed; a high degree of tailoring in terms of airworthiness and safety standards was required; the system safety program, as implemented, provided integration and synergism with the ongoing project; and no accidents or safety incidents had occurred in 3 1/2 years of operation.

The need for a rotor system test bed was recognized by both the Army and NASA in the 1960's. The establishment of a Directorate for the Army at several NASA Centers led to a combined NASA/Army effort to develop the RSRA through the normal process of concept studies, predesign studies, and finally a contract to build the aircraft in November 1973. The conceptual studies considered system safety, and a formal safety program was initiated when the specifications for the aircraft were established.

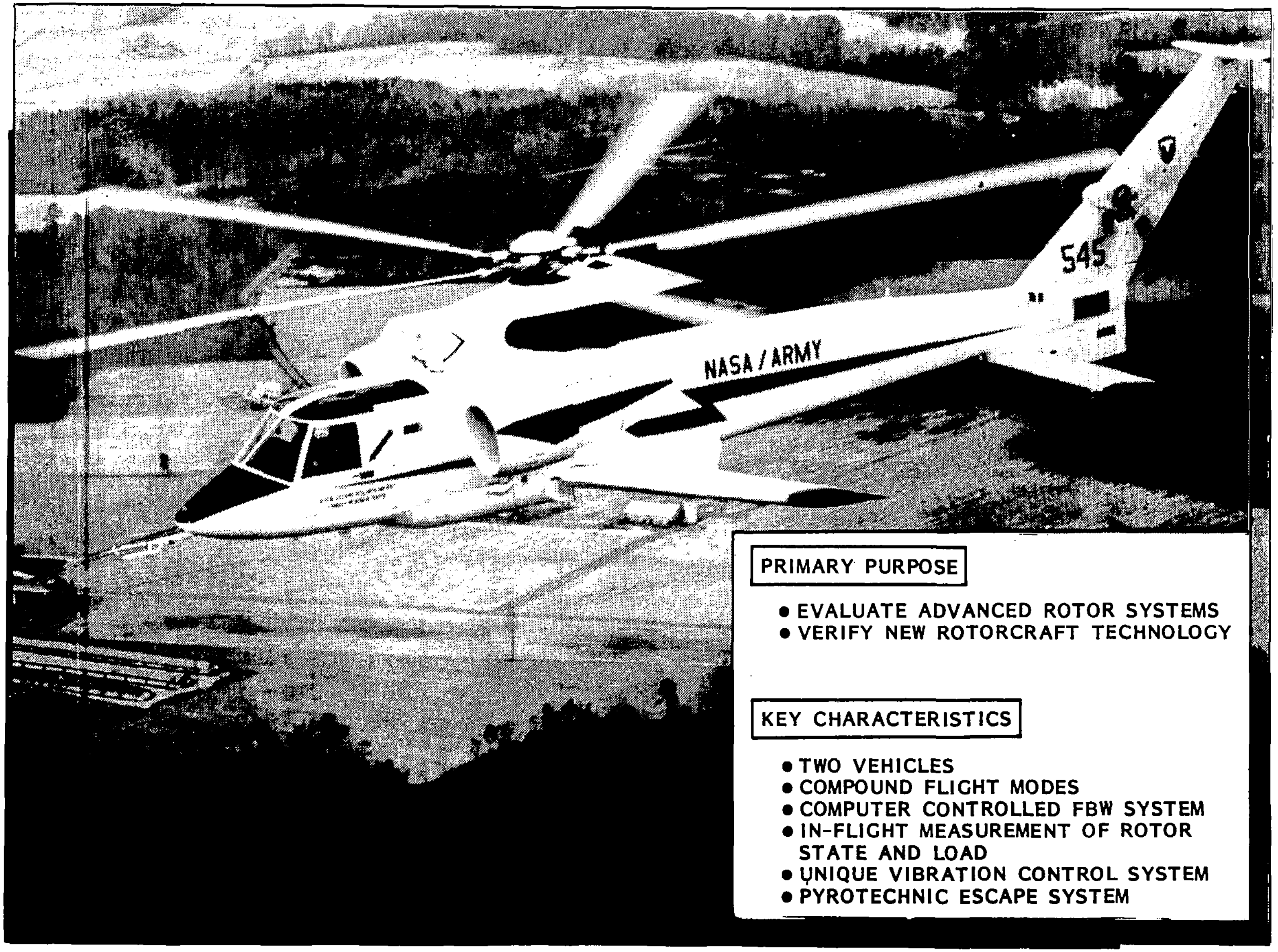


Figure 1.0-1 Rotor Systems Research Aircraft (Ames Research Center)

The RSRA project was initiated in 1973 to develop two research aircraft for evaluating advanced rotor systems and conducting rotorcraft flight research in a capable, efficient and cost-effective manner. The aircraft, shown in Figure 1.0-1, is a sophisticated test bed capable of flying as a helicopter, fixed-wing aircraft or combination thereof. It possesses systems and capabilities unique in the world of aviation, as illustrated in Figure 1.0-2.

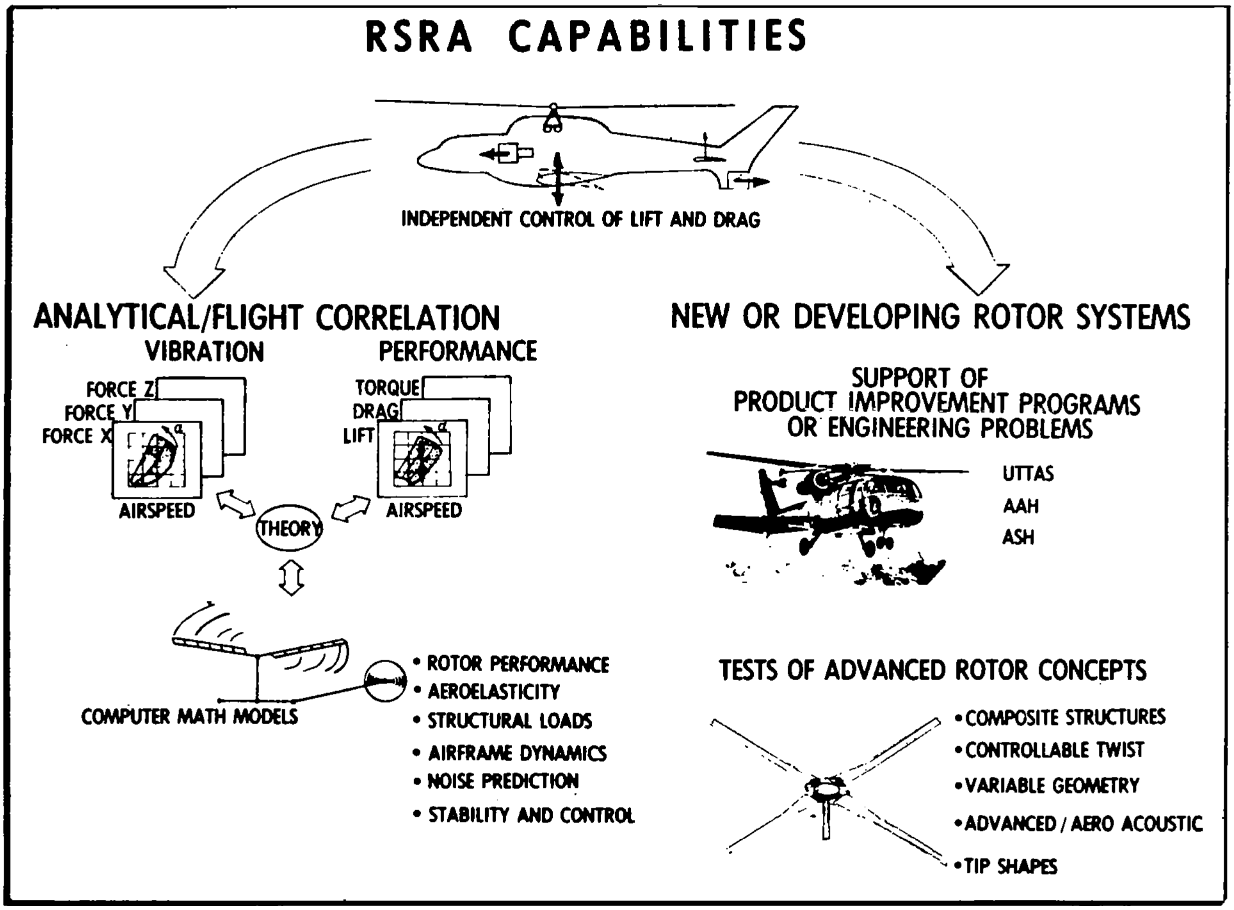


Figure 1.0-2 RSRA Systems and Capabilities

To provide an appreciation for the complexity of some of the safety issues that will be discussed, a detailed explanation of several of the unique safety systems of the RSRA is necessary.

a. Emergency Escape System (EES): Although escape systems are common on nonpassenger fixed-wing aircraft, no helicopter had ever been equipped with such a system. The auxiliary engines and the wing present obstacles to emergency escape "over-the-side" crew egress (Figure 1.0-3).

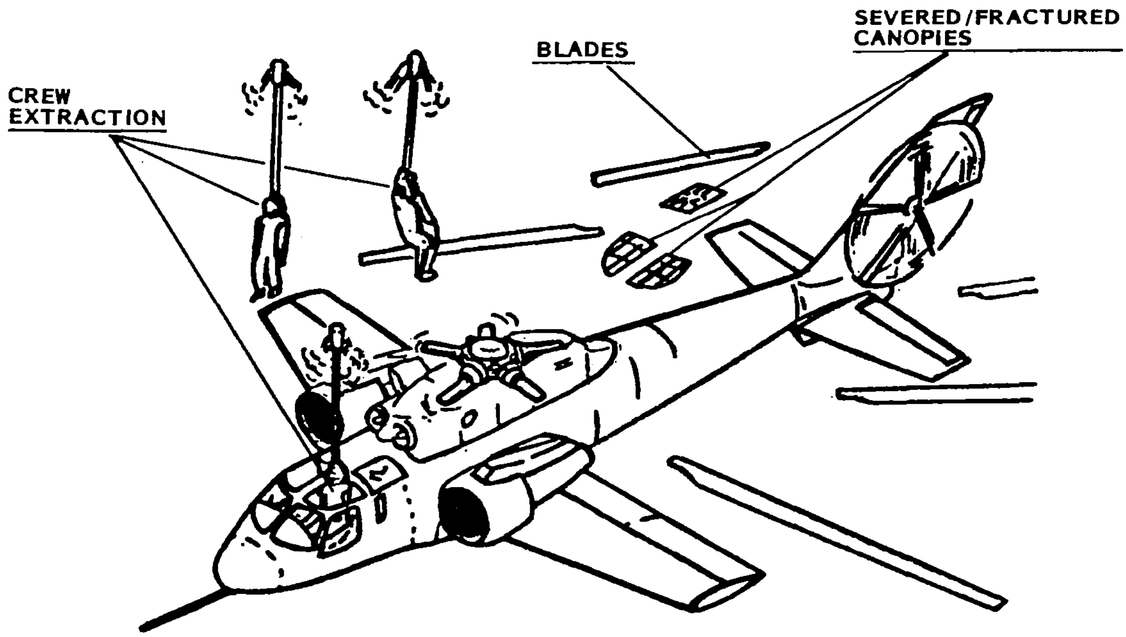


Figure 1.0-3 RSRA Crew Escape System

An EES is required to provide safe crew egress in an emergency such as fire, loss of control, or structural failure of a research rotor. The system provides for pyrotechnically severing the rotor blades, jettisoning and fracturing the canopies and extracting the crew members via tractor rockets. The blade severance system indexes the blades off sequentially in safe paths that avoid the aircraft and its flight path. The extraction system extracts crewmembers in a time sequence and trajectory path that provides separation from each other as well as from the aircraft structure. A static line extracts the parachute deployment bag, separates the crewmember from the seat back and initiates chute deployment. The system was qualified by a series of full-up sled tests and component tests. Transposing sled test data (with the sled constrained to the test track) to free maneuvering flight regimes was done by analysis. The resulting escape envelope covered zero/zero (zero altitude, zero airspeed) up to a modest cruise speed which was less than the maximum operational speed of the aircraft. The speed restriction resulted from a risk of entanglement of the deployment bag on aircraft structure in some combinations of aircraft attitude and postinitiation maneuvers.

b. Main Rotor Load Measurement System: A "six-component" wind tunnel type load cell balance system, as shown in Figure 1.0-4, is installed between the rotor and the airframe to provide a precise measure of the three forces and three moments imposed by the rotor on the airframe.

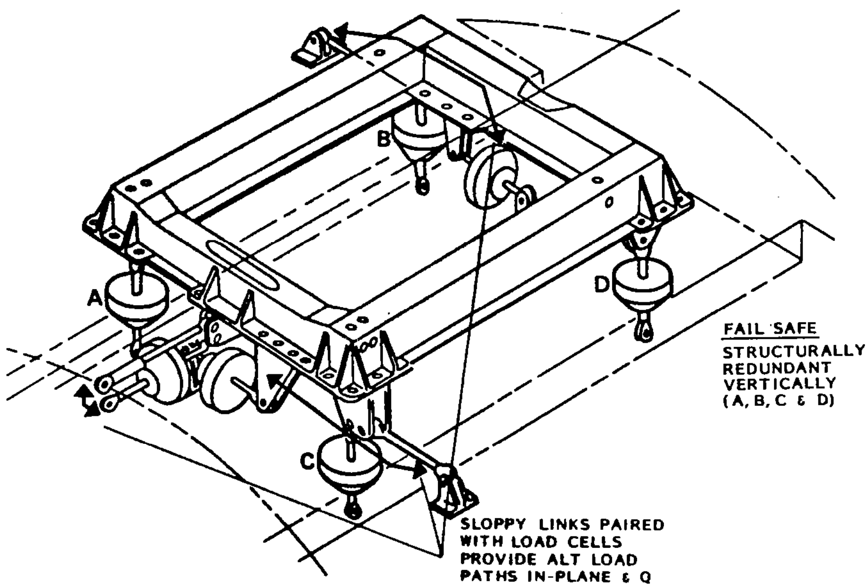


Figure 1.0-4 Main Rotor Load Measurement System

In actual implementation, a tradeoff is required between accuracy and structural integrity. For maximum accuracy and sensitivity, the load cells should be as thin as possible and there should be six load cells to fully define a statically determinant system. For maximum structural integrity, the members should be as "beefy" as possible and should be multiple redundant (such as by means of a 32-bolt circle attachment). The compromise was to provide redundancy via four vertical members, any three of which could carry design limit loads. Redundancy in the "in-plane" (lateral and fore & aft) direction was provided by "sloppy link" alternate load paths that pick up load when the system deflects a given amount on failure of any one load cell.

c. Active Isolation and Balance System (AIBS): An alternative main rotor load measurement system, Figure 1.0-5, is provided that not only measures loads but also isolates the airframe from "higher" frequency (3 to 30 Hz) rotor-induced vibratory forces.

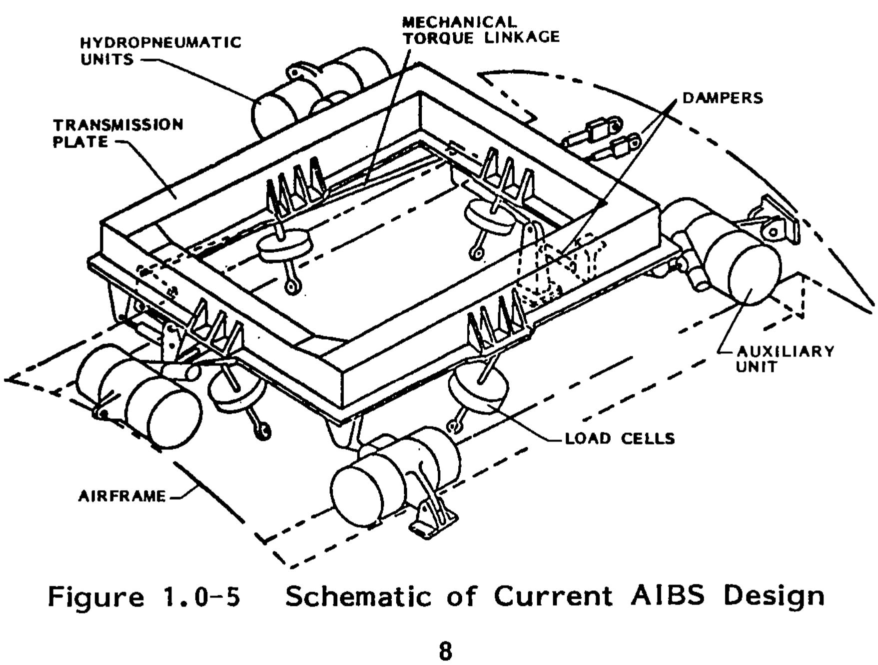


Figure 1.0-5 Schematic of Current AIBS Design

Structural integrity compromises were made to measurement system accuracy, similar to those made for the load cell system. The high vibratory force content of some of the candidate research rotors is such that vibration isolation is mandatory. When testing those rotors, the AIBS configuration would be used. In those cases, the first failure of the system had to be not only "fail-safe" (i.e. structurally adequate) but also "fail-operable" (i.e., continue to isolate high vibratory loads); thus, the need for the "auxiliary" isolator unit shown in Figure 1.0-5. As shown in Figure 1.0-6 the active isolator is effective in providing a 10:1 reduction in response to peak vibration modes at about 12 to 16 Hz.

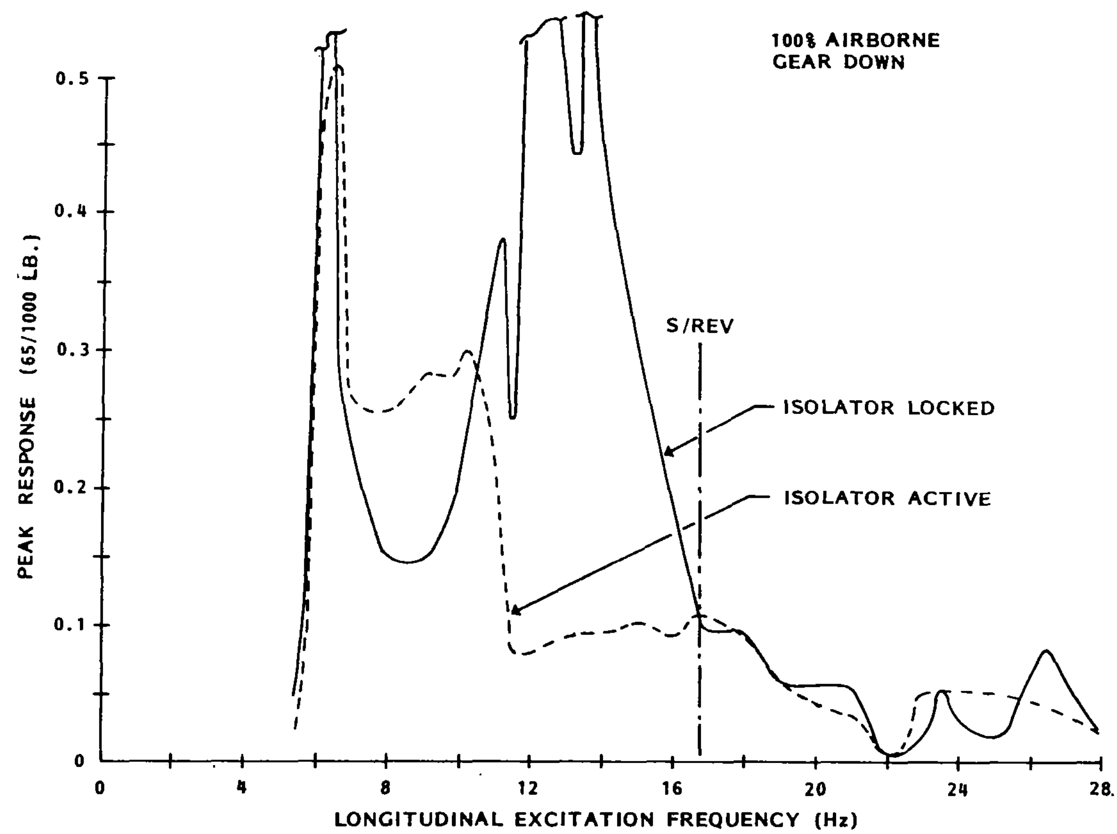


Figure 1.0-6 Isolator Effectiveness

d. Flight Control System: Two primary flight control systems are provided, with an additional onboard computer controlled Electronic Flight Control System (EFCS) and a Stability Augmentation System (SAS) as shown in Figure 1.0-7. The Safety Pilot's system is a relatively conventional hydromechanical boosted system; however, it is unique in that it provides actuation of both the fixed-wing airplane control surfaces (elevator, aileron, rudder) and the rotor swashplate controls. The control motions are split at a "Control Phasing Unit," which apportions motions to the fixed-wing and rotor controls in a pilot selectable schedule (i.e., 100 percent to both, 100 percent to one and 0 percent to the other, or any continuous combination of these). The Evaluation Pilot's controls are a "fly-by-wire" electrical tie-in to the Safety Pilot's hydromechanical controls through the Force Feel System. Both the EFCS and the SAS provide limited authority inputs to the flight controls, independent of any pilot-initiated commands.

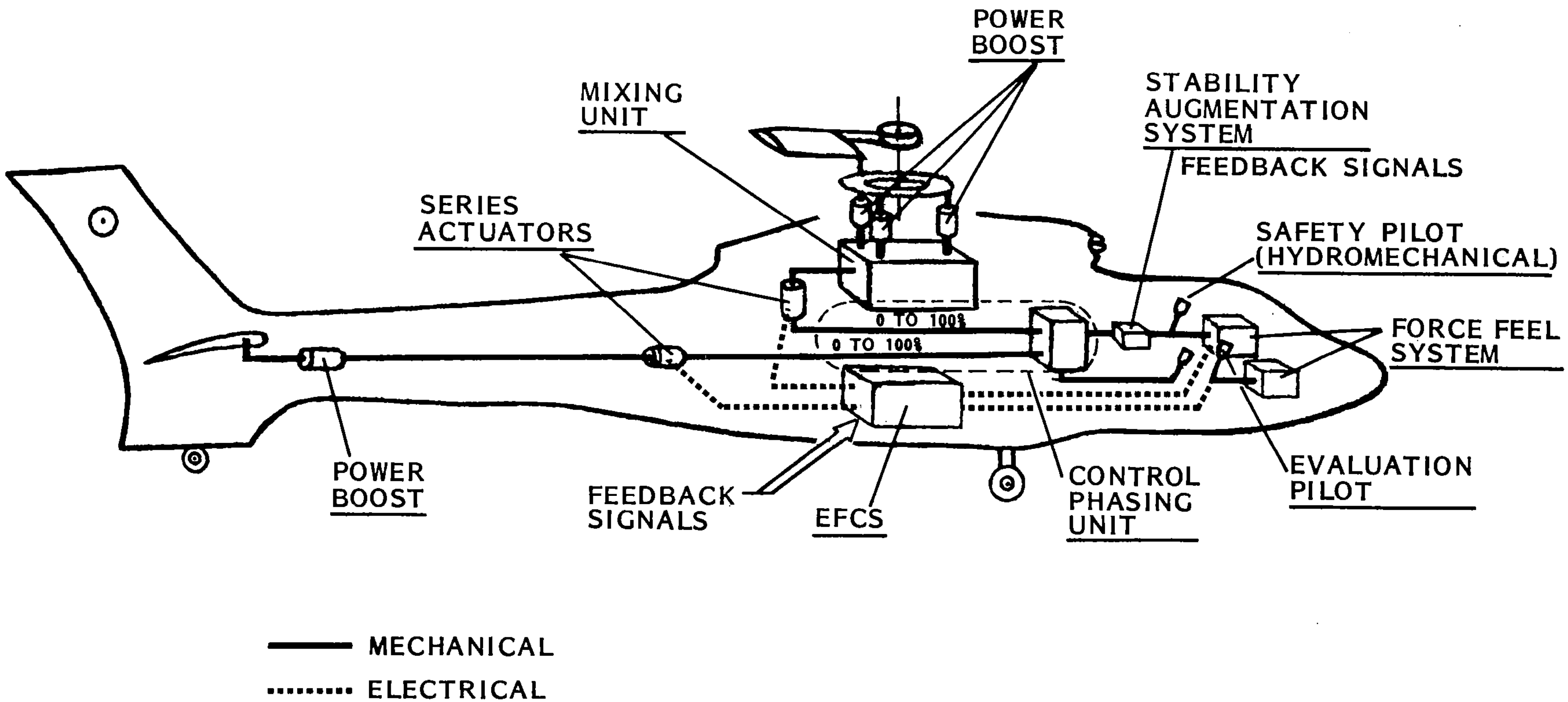


Figure 1.0-7 RSRA Flight Control System

This document presents the basis for project management use of safety and relates these management functions to "real-world" situations encountered on the RSRA project. In each example both the rationale which led to the safety-related project decision and the lessons learned as they may apply to future projects are presented.

2.0 PLANNING. The bases for RSRA project safety planning were:

a. Establishing the methods by which basic program risks could be identified.

b. Defining safety goals in terms of overall RSRA project goals.

c. Formulating specific project safety requirements.

d. Developing a detailed plan as an implementation guide for safety activities during product evolution.

2.1 RECOGNIZING PROJECT RISKS. The RSRA project management actively sought to identify and resolve project risks while recognizing both their moral and legal responsibilities. The moral responsibilities involved trust, image, reputation and the human desire to avoid injury to others. Legal responsibilities were perhaps more exacting. The potential consequences of failing to meet legal responsibilities were addressed by the RSRA project manager in briefings to the Langley Aviation Safety Committee. Questions were straightforward; e.g., "How would you, in your current role in this project, respond at an accident review board or in a court of law?" The legal issues involve the "feasances"; that is, in the event of an accident, penalties up to and including imprisonment may be levied upon conviction of negligence. Negligence typically involves malfeasance, wherein it is judged that problems, concerns, etc., were identified, but were ignored, and implementation of protective measures was deliberately avoided. Courts have been more lenient with respect to misfeasance cases wherein a hazard is identified and action is taken, or "reasonable" rationale for assuming the risk is provided within current technology. Thereafter, if an accident results, the effectiveness and reasonableness of actions and rationale may be questioned. Nonfeasance arises from the total lack of safety studies to identify hazards and subsequently to eliminate or control those hazards. Courts typically deal severely with such dereliction of duty.

Errors, failures, and unforeseen conditions do arise. Murphy lives; some even say he was an optimist. As potential undesired conditions are identified, additional concerns are normally revealed. Because of the likelihood of such a "domino" effect, project drivers were identified and addressed early, as illustrated by the following issues which are paraphrased from a memorandum written by the contractor project manager at the initiation of the project:

a. An escape system had never before been employed on a helicopter; however, because of the R&D nature of this project, such a provision was considered necessary.

b. An active isolation and balance system (AIBS) was necessary to isolate rotor vibrations from the fuselage. This system had only been demonstrated in one axis, and not in flight. The need for further testing and analyses was indicated.

c. Measurement accuracy requirements for the onboard research instrumentation (OBRI) were extremely tight. Operational data requirements and safety implementation called for the development and application of state-of-the-art instrumentation techniques.

d. The EFCS, which provided for a computer-controlled flight capability with a fly-by-wire backup system, was extremely complex.

e. Efficient technical interchange required close coordination between NASA and contractor project teams. The contractor, however, was concerned that this coordination might be uncomfortably close. On the other hand, NASA needed to be aware of technical progress as well as maintain surveillance over contractor activities in terms of schedules and contract resources. These conditions required formulation of communication protocols by NASA and contractor management.

Hardware, operational, and organizational issues were either directly or indirectly addressed in identifying potential project problem areas. This focused attention on critical issues early, thereby providing latitude in resolution concepts considered. Costly rework was minimized. Failure to do this early could cause compression of solution time, thus leaving designers "boxed in" as a result of firm designs in other areas. An important lesson learned is that early program-level risk identification is critical to system performance, cost, and schedule.

Resolution methods or acceptance rationale for identified risks on the RSRA project resulted from consideration of the three factors illustrated by the triangle concept. Real-world problems dictated tradeoffs between the factors shown in Figure 2.1-1, but a mutually acceptable balance was always maintained.

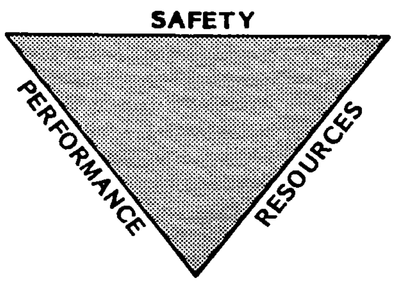


Figure 2.1-1 Typical Project Tradeoffs

Virtually every project decision impacted performance and resources, and frequently safety. Figure 2.1-2 is an example of NASA direction to reduce cost consistent with the required degree of safety. Safety analyses provided the management visibility to trade <u>on the basis of knowledge</u>.

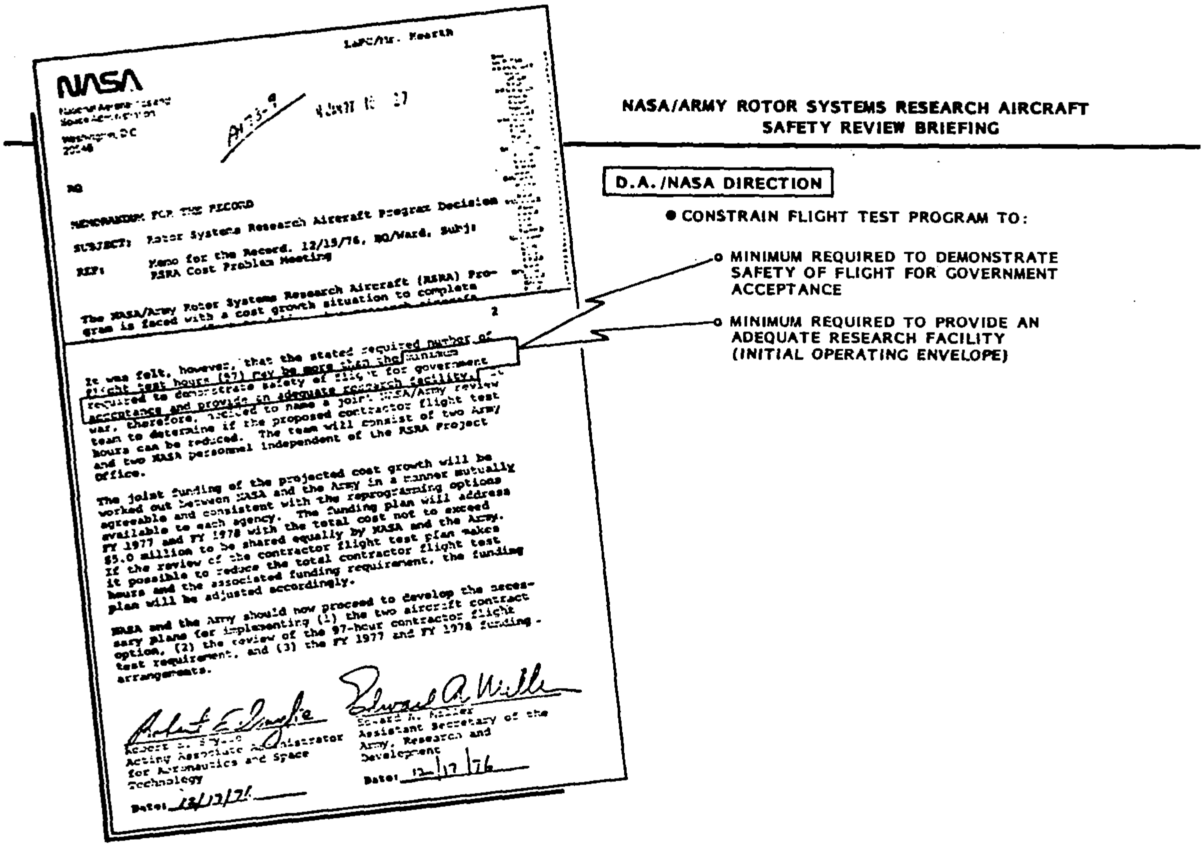


Figure 2.1-2 RSRA Cost Trade Example

2.2 SETTING PROJECT GOALS. Armed with an insight into safety risks and the necessity for a safety program, the next step was to create a plan to control it. The plan to manage safety was based upon project goals. The basic RSRA project goals, shown in Figure 2.2-1, reflect the concept that safety goals were an integral, balanced part of project goals. Project goals were neither overshadowed by safety nor was safety ignored.

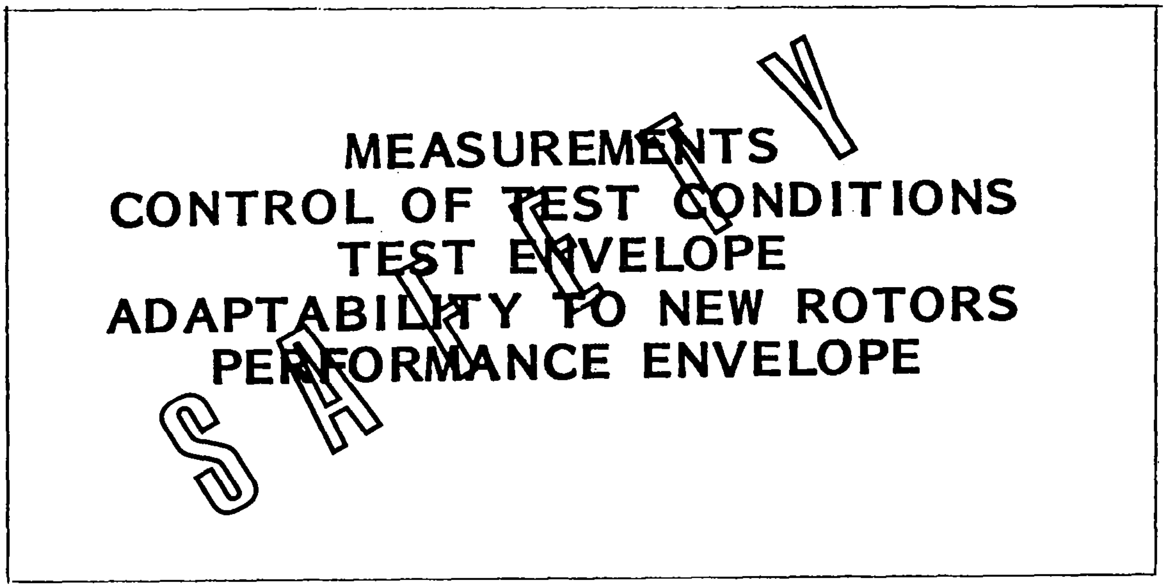


Figure 2.2-1 Priority Design Objectives - Presentation at Kickoff Meeting Reflected Integrated Safety Activity

The fundamental RSRA goals were directed toward producing a technically sound, safe aircraft. Each project goal encompassed general safety considerations.

a. Project goal: Provide an accurate measurement system to obtain experimental in-flight test data.

Safety consideration: Ensure appropriate balance between conflicting requirements for measurement system accuracy (high sensitivity; determinant) and structural integrity (high safety factors, implying lower sensitivity; redundancy, implying indeterminate structure).

b. Project goal: Provide precise control of test conditions.

Safety consideration: Ensure appropriate balance between precise control of test conditions (implying computer-controlled fly-by-wire system) and safety/reliability (implying inherent reliability of mechanical systems relative to electronic systems).

c. Project goal: Provide enhanced net lift and thrust test envelopes.

Safety consideration: Ensure that safety provisions were adequate for all test envelopes.

d. Project goal: Provide a vehicle which was adaptable to various rotor selections and configurations.

Safety consideration: Ensure that safety provisions were adequate for all hardware adaptations.

e. Project goal: Provide a performance envelope allowing operation over a wide speed and maneuverability range.

Safety consideration. Provide for operating personnel and public safety in all normal and predictable contingency and/or emergency modes.

These interdependent project and safety goals illustrate that safety is an integral part of mission accomplishment and also that mission/safety trade-offs are necessary. Early formulation of project and related safety goals sufficiently broad to encompass project activities is essential. If these early goals are too specific, however, tunnel vision may result.

2.3 SELECTING SAFETY REQUIREMENTS. "Requirements" are defined as those discrete actions necessary to achieve project goals. The set of safety requirements, viewed as a whole, addresses administrative authority, organization, tasks and timing, and system capabilities/limitations.

NHB 1700.1 (V3) states that "Safety goals and objectives should be established, and the type of system safety input that is to be furnished to the overall program should be determined . . . . It should be noted that these goals must be structured such that safety tasks can be selected that will accomplish the goals and when the tasks have been completed the results of the effort will clearly demonstrate that the goals have been met."

The RSRA safety goals related safety success to project success. Safety goals were established to describe how much safety was required or how much risk was acceptable.

The top level safety goals are shown below:

a. Protect the public.

b. Avoid project personnel accidents.

c. Prevent economic catastrophe.

d. Minimize operational problems.

The need to protect the public from hazards associated with the RSRA was paramount. Safety goals associated with this concern required consideration of potential crash landing situations; falling debris (e.g., severed rotor blades), and collision with military, commercial, or private aircraft.

Avoidance of project personnel accidents or injury involved consideration of hazards directly associated with the RSRA, its support equipment and its operation. The obvious RSRA project safety goal then was to identify and eliminate or control all potential causes for such hazards considering both mission and ground operations.

The third top level safety goal, to prevent economic catastrophe, was aimed at such events as loss of an aircraft (half of a two-aircraft fleet), destruction of high-value one-of-a-kind hardware, or occurrence of events reflecting unfavorably upon the developing Center or Agency which could result in loss of project funding.

The fourth goal, to minimize operational problems, dealt with such issues as schedule compliance and mission availability. This goal was the least significant for the RSRA project because of the minimal emphasis required on mission availability, as discussed elsewhere. Indirect safety implications of the effects of schedule and other operational problems, however, were not overlooked.

Based upon these goals, specific requirements were identified in terms of design characteristics, mission rules, operating procedures, personnel selection and training. Compliance with the requirements assured attainment of the goals. The requirements were met through performance of specific safety tasks using properly selected and tailored tools in accordance with the project schedule.

RSRA project safety task requirements and the timing of task performance were based upon an extensive review of other developmental aircraft programs and documentation governing the development and implementation of NASA and military safety programs. The RSRA task and timing requirements were tailored from the approach outlined in NHB 1700.1 (V3), shown below.

> It is anticipated that, in most cases, formal planning of the safety effort for support of the system feasibility studies would not be initiated. There are, however, several typical safety tasks that should be completed during these activities. These tasks then become the foundation for the planning of system safety efforts during the system definition, design, manufacture, test, and operation. These include:
>
> a. A review of pertinent historical safety data from similar systems.
>
> b. A continuing review of the gross hardware requirements and concepts, to maintain an understanding of the evolving system.
>
> c. A review of the proposed mission objectives.
>
> d. Completion of the planning for follow-on safety activities.
>
> e. The completion of preliminary hazard analyses to identify potentially hazardous systems and to develop initial safety requirements and criteria.
>
> f. Participation in trade studies with the results of the preliminary hazard analyses identifying highly hazardous areas, with recommendations as to the alternatives.
>
> g. Identification of the requirement for special contractor safety studies that may be required during system definition or design.

h. Estimation of gross resource requirements for the system safety program during the complete system life cycle.

i. Preparation of an index document that identifies all pertinent safety data developed during the life cycle of the system, such as the results of analyses, the criteria and requirements implemented, the results of special studies and the applicable historical data. This index is updated at the conclusion of each major increment of the system development or as determined by program milestone dates.

The specific tasks performed by the RSRA project are discussed in Section 2.4, and the project schedule and milestones are discussed in Section 2.4.6. The early definition of overall project safety tasks and their relationships with project goals and schedules was a key element in the safety success of the RSRA.

System requirements surveyed for the RSRA included the Federal Aviation Administration (FAA) Regulations, Air Force and Navy military specifications (including the MIL-A-8860 series), and Army documentation. Requirements from these sources were evaluated against unique aspects of the RSRA, which included the research and development nature of the project; its design, development test and evaluation aspects (i.e., strictly controlled flight environment and highly instrumented hardware); and the skill levels of the operational people who would be involved. Based upon these considerations, it was determined that Army document AMCP-706-203 (Engineering Design Handbook, Helicopter Engineering, Part 3 - Qualification Assurance) was the most appropriate. This was tailored paragraph by paragraph to the RSRA project.

Figure 2.3-1 presents examples of RSRA requirements compared to AMCP-706-203.

-RSRA Vs. AMCP-706-203: PROPULSION SYSTEM TEMP. SURVEY-

PARAGRAPH	706-203 REQUIREMENT	FULLY COMPLY?	RSRA PLAN/RESOLUTION
8.4.3.2 FLIGHT TESTS	TAKEOFF AND CLIMB TO MAX ALLOWABLE ALTITUDE	NO	OBTAIN CLIMB DATA TO 3000'
	LEVEL FLIGHT AT SELECTED ALTITUDES WITH POWER RANGING FROM HOVER (IGE & OGE) TO MAX	NO	HOVER IGE AT MAX WEIGHT; 120 KTS AT MAX WEIGHT UP TO 3000'; WORST CONDITIONS IN ENVELOPE
8.4.4 INSTRUMENTATION AND DATA ANALYSIS	TEMP MEASUREMENTS	NO	SEE 8.4.1
	TEST CONDITION MEASUREMENTS	NO	ALL EXCEPT ENGINE COMPARTMENT FLOW RATE - SIMILAR INSTALLATION TO S-67
	CORRECT TEMPS TO HOT ATMOS.	YES	NAS1-13000 TEMP LIMIT
	COMPARE DATA TO COMPONENT REQUIREMENTS	YES	DNE LISTING
8.4.5 DOCUMENTATION	PREPARE REPORTS TO INCLUDE:		
	- OPERATING CONDITIONS/DATA	YES	
	- SYSTEMS PERFORMANCE REVIEW	YES	AS REGARDS OPERATING LIMITS
	- OPERATING LIMITS IDENTIFIED	YES	

Figure 2.3-1 Comparison of RSRA and AMCP-706-203 Requirements

The yardstick applied to the RSRA was that it must meet a level of safety equivalent to the Sikorsky Model S-61 helicopter, which is an FAA certified transport category aircraft qualified for Presidential airlift. The requirements and the rationale for their selection were documented and included in the RSRA AQP.

The adaptation of an existing set of requirements to the RSRA project was effective and took maximum advantage of lessons learned on other programs. Serious errors of omission and commission can result, however, if extreme care is not exercised. A highly disciplined approach as illustrated by the Figure 2.3-1 example is essential.

2.4 DEVELOPING THE PLAN. The authoritative document of tailored safety guidelines for the RSRA project was the AQP. The AQP specified those engineering tests or analyses essential for substantiating the airworthiness of the RSRA. It presented concepts, schedules, and procedures for conducting design reviews for verifying adequacy of design for airworthiness, including safety. It specified prerequisites for reviews leading to safety-of-flight release prior to first flights by the contractor. Finally, it specified prerequisites for acceptance testing of the RSRA by the Government. The contents of the plan are shown in Figure 2.4-1.

Figure 2.4-1 RSRA Airworthiness Qualification Plan Table of Contents

Essential characteristics of the plan are described in the paragraphs below. Detailed discussions of the implementing organizations are provided in Section 3.0 and directing and controlling functions are treated in Sections 4.0 and 5.0, respectively.

2.4.1 Defining Requirements. After the project safety goals were developed, the actions required to achieve them were defined. In a similar manner, the requirements for achieving those goals were based on the RSRA design characteristics, the operational envelope, and mission scenarios. Thus, the ultimate mission of the RSRA was a major factor in defining the safety requirements. Recognition of this fact is illustrated in the AQP excerpt shown below:

> Concept of Operation and Maintenance. - The RSRA will be operated and maintained in a research environment by highly qualified experimental test personnel. Research instrumentation installed in the RSRA, together with NASA/Army data reduction and interpretation capability, will provide technical information necessary to monitor airworthiness of the aircraft. Planned service usage of the aircraft is 50 hours per year for 12 years, for a total of 600 flight hours per aircraft. Therefore, airworthiness substantiation requirements that assume world-wide operation and logistics support, in hostile natural or tactical environments, with a large fleet of aircraft accumulating many flight hours, do not apply to the RSRA. Selected airworthiness substantiation requirements that apply to the RSRA concept of operation are specified in this AQP.

Management attention to the ultimate mission of the RSRA permitted effective tailoring of the safety requirements and influenced safety-related decisions that occurred later in the project. The RSRA experience demonstrates the value of early identification and documentation of project requirements.

With the project requirements and safety goals clearly defined, the actions required to achieve the goals were developed and documented in the AQP. An excerpt from the AQP defines these actions:

> Each of the requirements listed hereunder shall be performed and verified during design reviews, prior to safety-of-flight release, or prior to acceptance test, as scheduled in Section 3.7. Verification of satisfactory fulfillment of these requirements shall be documented by the Government in an Airworthiness Qualification Report (AQR), which shall be issued as an Appendix to the AQP and which shall form the basis for the preflight review and safety-of-flight release. Each action item identified as a result of these requirements shall be specifically identified in the Airworthiness Qualification Report (Appendix A), corrective action shall be assigned and implemented, and adequate resolution verified by the Government, to provide a complete audit trail through the disposition of each action item. AMCP 706-203 is used as a guide in formatting the requirements of subsequent paragraphs herein, which

also specify government or contractor responsibility for compliance.

Several noteworthy items appear in the above excerpt: (1) Performance of tasks leading to fulfillment of safety requirements was correlated with the development schedule; (2) the requirement that specific safety activities be performed prior to design reviews and scheduled tests directed the allocation of resources for timely completion; and (3) this integrated approach is an essential ingredient of a successful safety program.

Another significant item is that compliance with each requirement had to be sufficiently documented to provide an audit trail. All action items generated to satisfy the requirements, and steps taken to resolve each action item, were recorded in a single document, the AQR. Responsibility for entering concerns and their resolutions in this document rested with the project office. Action items resulted when identified hazardous conditions compromised the basic RSRA safety goals. The potential for compromising goals was determined by categorizing identified hazards as shown below.

Category I - Conditions such that a malfunction will cause subsequent equipment loss and/or death or multiple injuries to personnel.

Category II - Conditions such that a malfunction requires immediate corrective action for personnel or equipment survival, or that will result in being one failure removed from a category I situation.

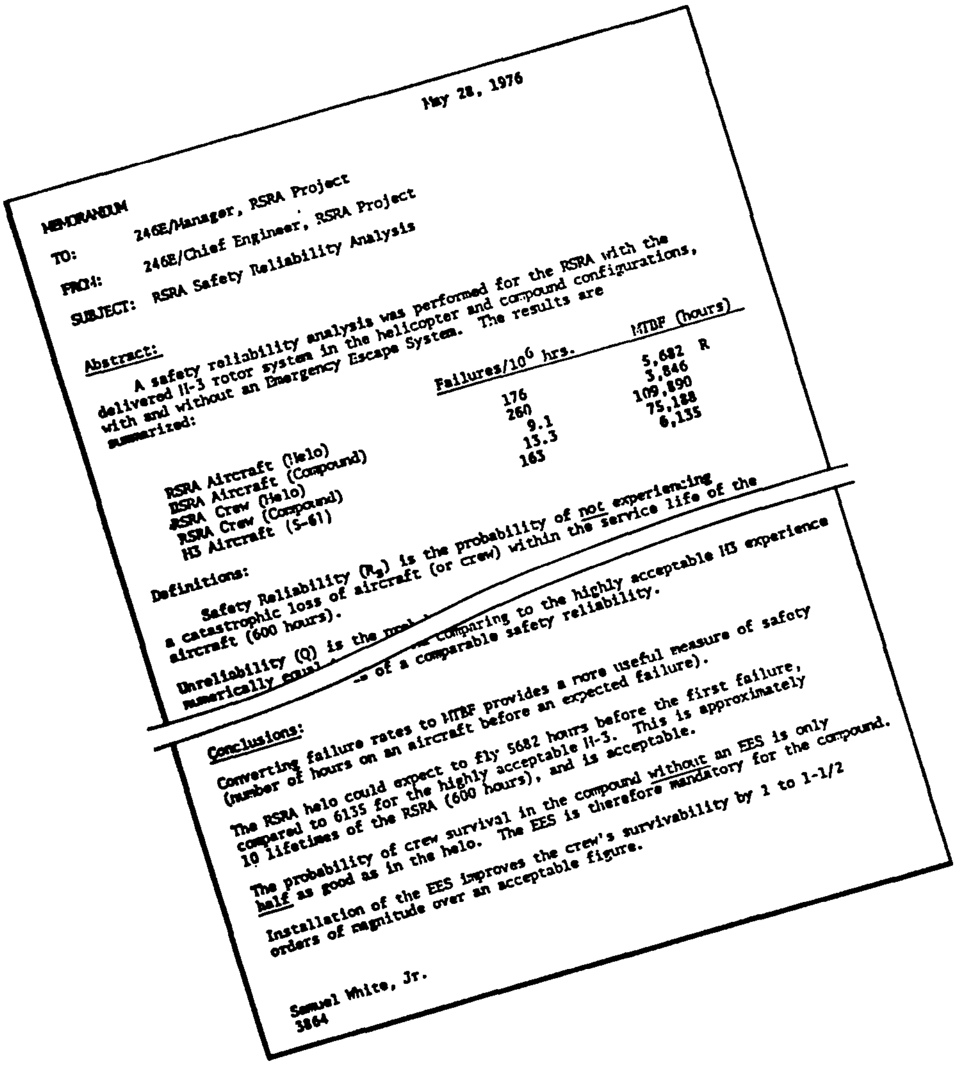
Category III - Conditions such that a malfunction will degrade performance but can be controlled without major damage or any injury to personnel.

Category IV - Conditions such that a malfunction will not result in major degradation and will not produce equipment damage or personnel injury.

Since hazards in categories I and II involved the potential for loss of life; the elimination or control of these hazards was required to achieve the RSRA safety goals. Elimination through design was not feasible in all cases, so it was necessary to provide alternate solutions. The "safe life" concept was employed whereby statistically representative samples were tested to predict the safe useful life of critical systems based on the concept that catastrophic failure modes existed and had finite probabilities. The "safe life" concept was applied to category I hazards. This precaution, together with emergency provisions, provided the most safety consistent with mission requirements. Category II hazards, one failure removed from category I, which could not be completely eliminated through design were addressed via redundancy and special procedures.

Fail-operational provisions necessary for satisfying project requirements were aimed at sustaining a failure and still allowing minimum mission objectives to be met. Design and safety requirements were not concerned only with single and dual failures. Fail-operational (i.e., continue operational following two failures) requirements were specified when component unreliability, environmental conditions and aircraft operating characteristics so required. More detailed discussions of implementation of these concepts are provided in Section 4.4.

The rigorous approach described above was not warranted in all cases. Another method employed on the RSRA for verifying that a requirement had been met was to refer to a previously demonstrated safe system or configuration. Comparison of the RSRA to the demonstrated "safe" H3 (S-61) aircraft is an example of this method. Figure 2.4-2 shows some of the exhaustive comparisons made between the two vehicles.



May 28, 1976

MEMORANDUM

TO: 246E/Manager, RSRA Project

FROM: 246E/Chief Engineer, RSRA Project

SUBJECT: RSRA Safety Reliability Analysis

Abstract:

A safety reliability analysis was performed for the RSRA with the delivered H-3 rotor system in the helicopter and compound configurations, with and without an Emergency Escape System. The results are summarized:

	Failures/10^6 hrs.	MTBF (hours)
RSRA Aircraft (Helo)	176	5,682 R
RSRA Aircraft (Compound)	260	3,846
RSRA Crew (Helo)	9.1	109,890
RSRA Crew (Compound)	13.3	75,188
H3 Aircraft (S-61)	163	6,135

Definitions:

Safety Reliability (R_S) is the probability of not experiencing a catastrophic loss of aircraft (or crew) within the service life of the aircraft (600 hours).

Unreliability (Q) is the ... comparing to the highly acceptable H3 experience numerically equal ... of a comparable safety reliability.

Conclusions:

Converting failure rates to MTBF provides a more useful measure of safety (number of hours on an aircraft before an expected failure).

The RSRA helo could expect to fly 5682 hours before the first failure, compared to 6135 for the highly acceptable H-3. This is approximately 10 lifetimes of the RSRA (600 hours), and is acceptable.

The probability of crew survival in the compound without an EES is only half as good as in the helo. The EES is therefore mandatory for the compound.

Installation of the EES improves the crew's survivability by 1 to 1-1/2 orders of magnitude over an acceptable figure.

Samuel White, Jr.
3864

Figure 2.4-2 RSRA Safety/Reliability Analysis Report

Caution should be exercised, however, when qualifying systems or components by similarity. The similarity must apply not only to the hardware, but to its intended use by operating personnel, within the specified environments, and with other systems.

In addition to the requirements imposed directly by the AQP, do's and don't's for safety, reliability, and maintainability were contained in the design guides which were part of the System Requirements Handbook delivered and reviewed at the Preliminary Design Review (PDR). These documents, provided by the contractor, provided excellent technical reference material developed specifically for this project and included data derived from many years of helicopter experience. The System Requirements Handbook provided a very useful standard against which to substantiate that the RSRA met system and project requirements and was ready for research operations.

The planning in the AQP led logically to the identification of specific safety tasks which, when accomplished, satisfied the requirements.

2.4.2 Identifying Safety Tasks. The safety tasks performed on the RSRA project were structured to meet the requirements imposed by the AQP which, when satisfied, ultimately led to achievement of project goals.

Basic safety tasks outlined in NHB 1700.1 (V3) are shown below:

Identify the hazards in the system.

Determine corrective actions that may be implemented to either remove or control the hazard or to provide alternatives.

Recommend corrective action or alternatives to the appropriate management level for a decision to either resolve the hazard or assume the risk.

Document those areas in which a decision has been made to assume the risk, including the rationale for the risk assumption.

Specific safety tasks for the RSRA project were defined on the basis of these basic tasks and were documented in the AQP, as shown below.

SYSTEM SAFETY:

Hazard Analysis. - Contractor responsibility to perform system, subsystem and operating hazard analyses in accordance with contract NAS1-13000, Supplement VI, Section 4.6, to identify and categorize hazards. Objectives of reviews shall be to eliminate, reduce to an acceptable level, or otherwise resolve any Category I and II hazards that are identified.

Contract Documentation. - Contractor responsibility to submit and update catalogue following Preliminary Design Review (PDR) and final Critical Design Review (CDR), and prior to Flight Readiness

Review (FRR) and Pre-Flight Review (PFR) as specified in contract Supplement VI, Section 4.6 and as scheduled in the documentation requirements of supplement III.

Corrective Action. - Government responsibility to incorporate as action items in the AQR a list of all Category I and II hazards identified; also, to review corrective action, verify acceptable resolution of the hazard, and document corrective actions and final resolution in the AQR. Conduct a safety review concurrently with each program review specified in Section 3.2. Responsibility - Rotor Systems Research Aircraft Project Office (RSRAPO), chief engineer.

Safety Surveillance. - Government responsibility to monitor contractor program and identify as action items any additional hazards reported in accident/incident reports, quarterly audits, hazard notification sheets, or hazard catalogue. Document in the AQR all hazards identified, corrective actions and resolution. Responsibility - RSRAPO chief engineer.

These tasks were tailored to the project in that selection, scope, and depth were limited to that necessary and sufficient to demonstrate safety adequacy. Performance of these tasks supported the milestone schedule discussed in Section 2.4.6.

This approach to accomplishing tasks was effective on the RSRA project. Exceptions taken to plan implementation in this area are discussed in Section 4.0.

A word of caution relative to task selection and definition is that contracts should be scrutinized closely to ensure that necessary tasks are properly scoped and requirements imposed. The decision to exclude specific systems, subsystems, or operations should be made only if solid rationale for the exclusion is provided and documented.

2.4.3 Establishing Safety Accountability. Establishment of safety goals, development of requirements enabling achievement of those goals, and definition of implementing tasks were discussed in the preceding sections of this document. Responsibility, or more precisely, accountability, for task accomplishment leading to goal achievement involved the line organization, but also brought to bear other Center and NASA elements.

Responsibilities and assignments were specific and assignees were held accountable for the adequacy, accuracy, and timeliness of their products. In short, everyone knew where the buck stopped.

The RSRA AQP outlines those accountabilities.

ORGANIZATION AND RESPONSIBILITY:

RSRA Project Office. - The NASA/Army Project Office is responsible for performing Government tasks defined herein and for documenting in the AQR each item of compliance or action requirement. As assigned by each paragraph above, the RSRAPO will monitor contractor activity, review contractor documentation, verify compliance with contract requirements and program objectives, identify action items requiring resolution, and approve final disposition of action items and documentation. RSRAPO will further provide data for the AQR documenting compliance with contract and program requirements and problem resolution. Specific RSRAPO responsibilities are assigned in Table 1.

Langley Research Center (LRC) - Aviation Safety Officer (ASO). - The Langley ASO is responsible for verifying that the RSRA is airworthy, based on the data presented in the AQR and at project reviews. At the conclusion of PFR he will confirm that each prerequisite has been met and each open item resolved, with support from the RSRAPO, the Langley Aviation Safety Committee, and the RSRA Project Review Panel, as required. He will chair review teams at FRR, and PFR and will submit a memorandum documenting review determinations and findings, including recommendation for safety-of-flight release, for approval by the Director, Langley Research Center.

Review Team Chairman: The chairman of other review teams will identify airworthinesss action items in the AQR, as required. RSRAPO cognizant WBS Managers will assure entry of action items in the AQR and verify disposition.

Surveillance of the contractor program, as well as review, verification, and documentation of corrective actions as shown above were the responsibility of the RSRA Chief Engineer.

The distribution of accountabilities as described in the AQP was very effective on the RSRA project. The key to the success of the plan was the assignment of accountability high enough in the organizational chain to provide sufficient muscle to achieve assigned tasks. Implementation of that plan is discussed in Section 4.0, Directing, and illustrated in Figures 3.2-1 and 4.1-1.

2.4.4 Defining Safety Tools. The safety plan defines the safety tools to be used. Typical hazard identification tools are discussed in NHB 1700.1 (V3) and other references. These include many forms as outlined in Figure 2.4-3.

RANDOMLY

- SCENARIOS
- DELPHI APPROACH

SYSTEMATICALLY

- HAZARD ANALYSIS (CONCEPTUAL, SYSTEM/SUB-SYSTEM, OPERATING, DECOMMISSIONING)
- FAULT TREE ANALYSIS
- SNEAK ANALYSIS
- MANAGEMENT OVERSIGHT RISK TREE
- OTHER SPECIAL STUDIES (FMEA, ETC.)

Figure 2.4-3 Approaches to Hazard Identification

Based on an understanding of project goals and experience with developmental aircraft, it was concluded that individual subsystem hazard analyses, a system hazard analysis, and an operating hazard analysis would be sufficient to cover the spectrum of safety requirements. From that premise, RSRA project management selected techniques from the relatively extensive menu of methods available for accomplishing hazard identification, and imposed the requirement for their use, as stated in Section 2.4.2. A discussion of the actual application of these tools is provided in Section 3.1.

Additionally, a contractual requirement existed for performance of failure modes and effects analyses (FMEA's). Generally, FMEA's are recognized as reliability rather than safety tools. Previously prepared FMEA's can be used effectively in safety assessments by adding failure criticalities. This produces a Failure Mode Effects and Criticality Analysis (FMECA) as was done on the RSRA project. The intended mission of the aircraft made maintainability and mission availability very minor factors. Consequently, the thrust of the FMEA's was redirected toward hazard identification rather than probability of failure determinations needed for availability and maintainability analyses. FMEA's were also useful in determining the potential safety impact of failures which occurred during testing. These applications of FMEA's on the RSRA proved very effective.

This judicious FMEA tailoring is supported and indeed recommended by NHB 1700.1 (V3) which states in part:

> The analysis methods may be expanded, reduced or altered as required to suit the specific needs of any separate program, or initiated during any time in the system development, thus assuring maximum flexibility.

This concept reflects the certainty that all project performance and resource problems cannot be anticipated several years ahead of time. A notable feature of the AQP was that flexibility was provided to use additional safety tools or modify existing ones as the need was identified. This flexibility was exercised repeatedly throughout the project.

2.4.5 Providing Information Flow. The RSRA project implemented a disciplined approach to information flow through the use of formal design reviews. These reviews served to evaluate current status of aircraft development and to disseminate required information to all organizations. As can be seen in the excerpt from the AQP shown below, safety activities were included in the design evaluation at the same level as hardware development activities.

> Concept of Project Reviews. - Preliminary Design Review (PDR) and Critical Design Review (CDR) will be conducted by subsystem (WBS level 3), immediately preceding design reviews of the Air Vehicle System (WBS level 2), as scheduled in figure 1. The review will be conducted at the contractor's facility or other location(s) agreeable to both the Contractor and the Government. Systems Engineering and Test and Evaluation elements will be incorporated into design reviews as they pertain to the system or subsystem under review. Flight Readiness Review (FRR) and Pre-Flight Review (PFR) will be primarily devoted to Airworthiness and safety-of-flight considerations. Pre-Acceptance Test Review (PATR) will be primarily devoted to RSRA system capability and readiness for research operations. Concepts of each review are summarized as follows: . . . .

This planning illustrates the safety awareness of the RSRA project management.

After each formal design review, the review chairman prepared a report to the RSRA project manager identifying action items and stating recommended resolutions. In addition, the review team chairman assigned actions which required systematic documentation as discussed in paragraph 2.4.3. These documentation procedures ensured that project management was aware of the risks involved and of the rationale associated with those risks. The documentation also provided an audit trail.

The flow of technical information was augmented in a less formal way at the weekly (each Monday morning) staff meetings. WBS managers presented their actual status compared to planned status and discussed problems encountered and the outlook for their work areas. It was necessary that they coordinate closely with their contractor counterparts to be up to speed at those meetings. A joint NASA/Army management meeting was held monthly along similar lines, but with high level managers. One attempt to combine these two meetings was singularly unsuccessful because of the inhibiting effects of the presence of higher level managers. An important lesson learned from these meetings was that they should be held at the lowest level possible, consistent with the authority required. Discussion of problem areas tended to be suppressed in the presence of too much horsepower.

Both the formal and informal methods for dissemination of information were effectively used on the RSRA project. The effectiveness of both methods was enhanced by establishing schedules which permitted timely generation and interchange of the required data.

2.4.6 Scheduling Project Milestones. The coordination of safety and development activities was accomplished as planned in the AQP. The AQP identified the significant project milestones, the input data required, and the information to be delivered. Representative items considered were:

a. AQP release and revisions.

b. Initiation of each type of hazard identification analysis.

c. Completion of each type of hazard identification analysis.

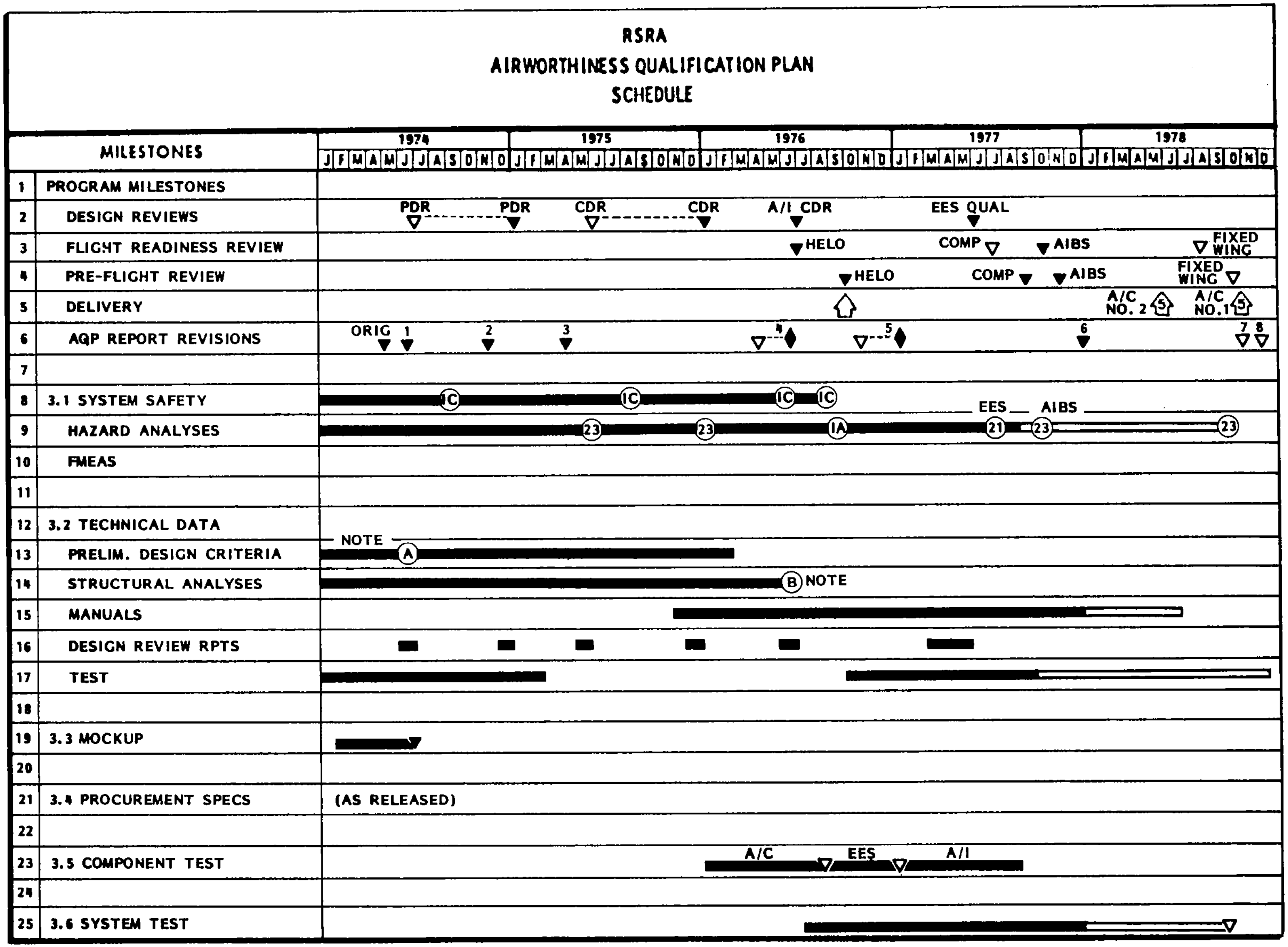
d. A schedule of major reviews.

The safety milestones appeared on the official project schedule as shown in Figure 2.4-4, and were clearly related to the project phases and major events.

This approach kept safety in perspective. That is, an awareness of safety issues was maintained without overkill. It is concluded from the RSRA experience that safety activities contribute to project success when they are included in the mainstream of project activities and proper emphasis is maintained.

2.4.7 Providing Safety Education. Safety education, training, and advisories were planned and provided as RSRA project changes dictated. The need for extra training came about as a result of transfer of operations from Wallops Island, Virginia, to Ames Research Center, California, resulting in general loss of corporate memory. Because of the "experimental shop" approach to documentation, incomplete transfer of personnel, and changed operational missions and roles, an aggressive training program was required.

New personnel on the RSRA project had little specific previous system safety experience. Implementation of the RSRA project safety plan depended upon understanding and acceptance on the part of project personnel. Specific training was provided to staff personnel in a timely fashion to support overall project schedules. Training was tailored in terms of the orientation, technical need, and complexity of the program. An outline of one of the safety seminars presented at Ames is shown in Figure 2.4-5.



A - AERO, STABILITY, FLIGHT CONTROLS, STRUCTURAL CRITERIA, WEIGHT BALANCE, DESIGN SPEC REPORTS (2,2A, 2B, 3, 4)
B - AIRFRAME, LANDING GEAR, LOADS, FLIGHT CONTROLS, SYSTEM REQUIREMENTS (30, 30A, 30C, 30D, 30E, 30F, 30G, 13)
1C - COMPLETION OF SUBSYSTEM/SYSTEM HAZARD ANALYSES
23 - COMPLETION OF FMEA'S

NO'S IN CIRCLES REFER TO CONTRACT SUPPL III DATA ITEMS.

Figure 2.4-4 Airworthiness Qualification Plan Schedule

SYSTEM SAFETY SEMINAR OUTLINE

1. SEMINAR OBJECTIVES :

(ME) .... INFORM		- WHAT IS SYSTEM SAFETY? - HOW CAN IT BE ACHIEVED?
(YOU) ..... UNDERSTAND		- REQUIREMENTS FOR AN EFFECTIVE SYSTEM SAFETY PROGRAM - TECHNIQUES FOR PLANNING AND IMPLEMENTING
(WE) .... CREATE		- SAFETY ATTITUDE - SENSITIVITY TO AND AWARENESS OF RISKS/HAZARDS
(WE) .... DEVELOP		- AN EFFECTIVE SYSTEM SAFETY PROGRAM PLAN - AN EFFECTIVE SYSTEM SAFETY PROGRAM - AN EFFECTIVE DIVISION SAFETY PLAN

2. CONCEPTUAL DEFINITIONS
3. ASSESSMENT (CURRENT SAFETY SITUATION)
4. BASIC PRINCIPLES
5. SYSTEM SAFETY TASKS
6. RISK MANAGEMENT
7. PREVENTABLE ACCIDENT CASE STUDY
8. SAFETY PLAN - HELICOPTER TECHNOLOGY DIVISION
9. RESEARCH AIRCRAFT SYSTEM SAFETY PROGRAM PLAN

Figure 2.4-5 RSRA System Safety Seminar Outline

3.0 ORGANIZING. The RSRA AQP provided the framework for organizing project functions and personnel within the context of the schedule. The project manager assembled those elements and incorporated such intangibles as technical competence, safety attitude, and motivation to produce a flexible, efficient, integrated team.

3.1 ORGANIZING THE WORK. The work elements of the safety program within the project organization included controlling the configuration, selecting and applying tools for hazard identification, and reviewing the results of safety activities.

3.1.1 Controlling Configuration. The RSRA project used the experimental shop approach to configuration control, as shown by the Figure 3.1-1 directive, wherein the control process consisted primarily of red-lining the drawings and in some cases changing them to conform to the as-built configuration.

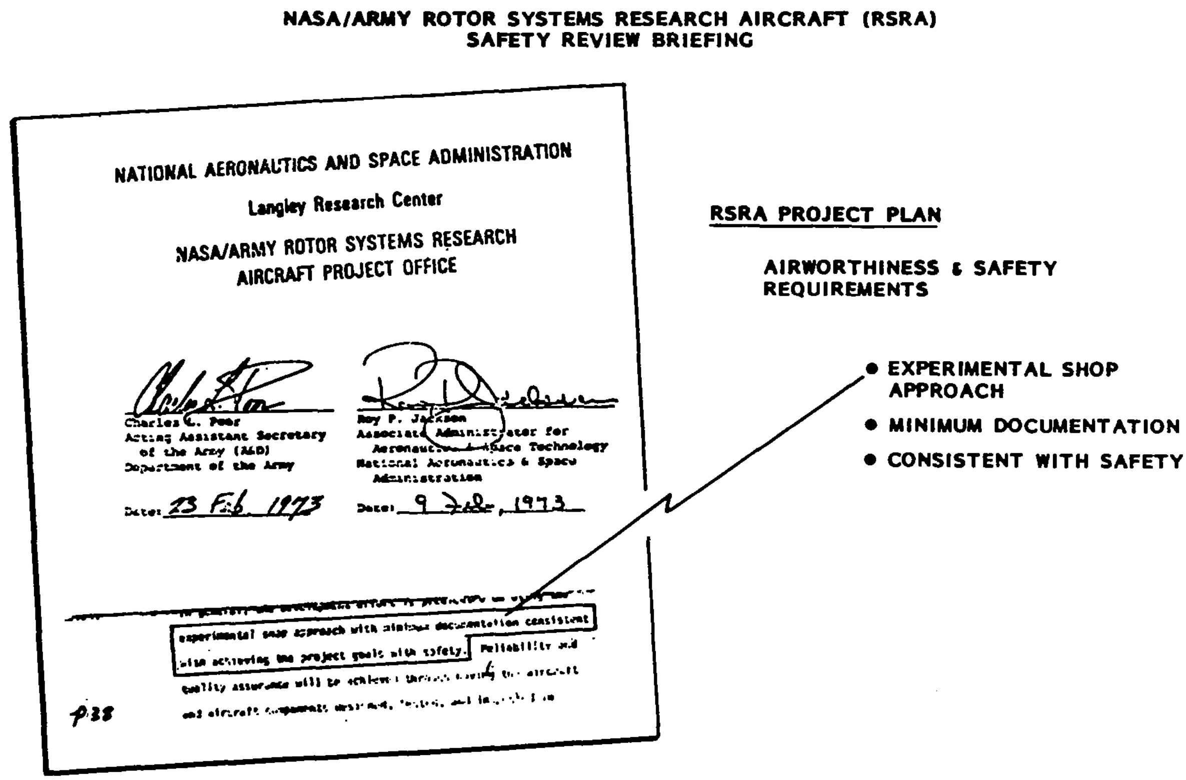


Figure 3.1-1 RSRA Experimental Shop Approach Direction

Signature authority under these conditions was extremely important. Approval of all drawing changes required the signature of the Project Chief Engineer and the chief of quality control. Project success in this area depended largely on the close working relationships between the project staff and contractor personnel, augmented by the conscientious attitude of all involved. A problem resulting from this experimental shop approach is discussed in Section 6.0. A lesson learned from this RSRA experience is that without unusual dedication and cooperation on the part of project participants, serious program level problems can result. If program dollars are a driver and minimum configuration control and documentation requirements are levied, it is imperative that essential documentation be defined and a requirement for its delivery imposed. NASA document JSC 07700, Volume IV, "Configuration Management Requirements," is an excellent reference.

3.1.2 Selecting Tools. Tools were selected for performance of the safety tasks after the configuration was defined. This applied whether the configuration dealt with a concept, the hardware, or an operation.

Initial tool selection was based upon the intent of the AQP; i.e., each subsystem, its interaction with the total aircraft system, and aircraft operations were evaluated. The chronology in Figure 3.1-2 below shows the tools employed and the major project events supported.

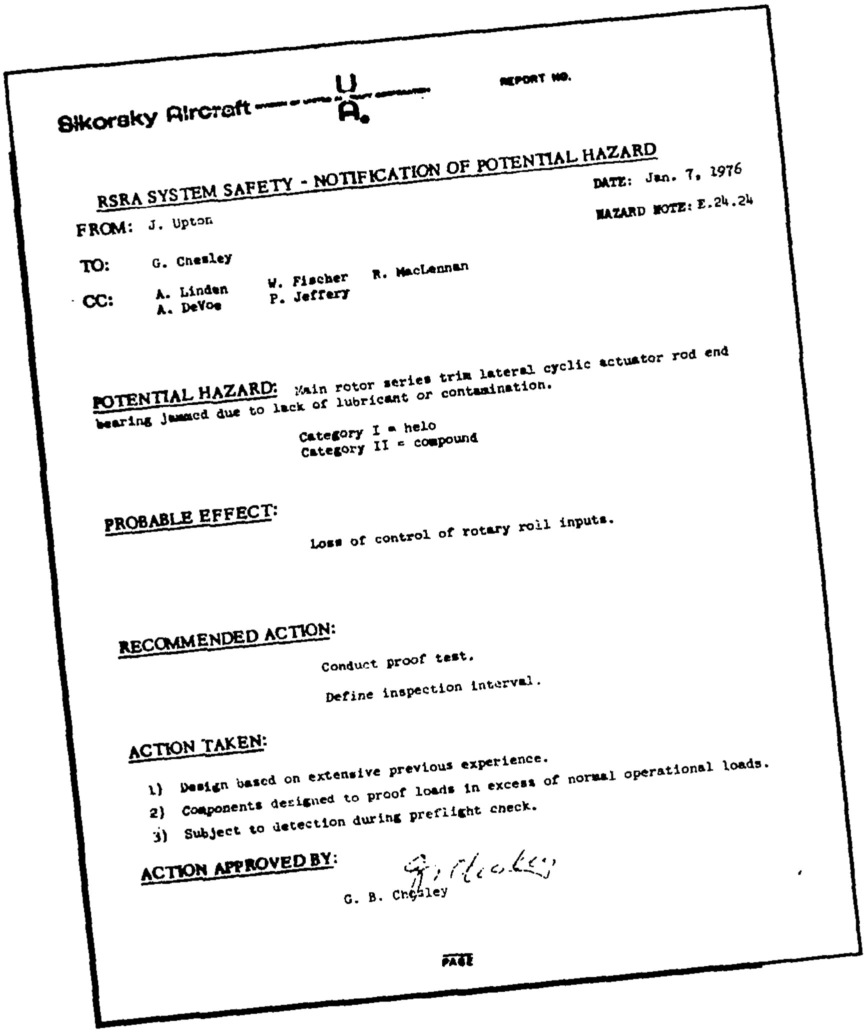
SUPPORTED	DELIVER FAILURE MODE AND EFFECTS ANALYSIS (FMEA) (EXCEPT ACTIVE ISOLATION AND BALANCE SYSTEM AND EMERGENCY ESCAPE SYSTEM)	5/75
RESPECTIVE	DELIVER PRELIMINARY HAZARD ANALYSIS (PHA)	1/76
PDR's and CDR's	REVIEW OVERBEY REPORT	5/76
	DELIVER FMEA AND HAZARD CATALOGUE (VICE SYSTEMS, AND SUBSYSTEMS HAZARD ANALYSES)	7/76
	FLIGHT READINESS REVIEW (FRR)	7/76
	AIRCRAFT DELIVERY	7/76
	PRE FLIGHT REVIEW (PFR)	10/76
	SAFETY OF FLIGHT RELEASE (SOFR)	10/76
	DELIVER FMECA FOR ACTIVE ISOLATION AND BALANCE SYSTEM	7/77
	DELIVER FMECA FOR EMERGENCY ESCAPE SYSTEM	1/78
	DELIVER FAILURE MODE EFFECTS AND CRITICALITY ANALYSIS (FMECA), FINAL	10/78
	DEVELOP TOP LEVEL FAULT TREE	1980
	PREPARE ELECTRONIC FLIGHT CONTROL SYSTEM (EFCS) FAULT TREE	1980
	DEVELOP EFCS COMMON CAUSE FAILURE ANALYSIS (CCFA)	1980
	DEVELOP EFCS SNEAK CIRCUIT ANALYSIS (SCA)	1980
	UPDATE EFCS FMECA UPDATE	1980

Figure 3.1-2 RSRA Project Events and Supporting Safety Tasks

Some subsystems were excluded from the analysis effort based upon either a previously proven track record or similarity to other subsystem or aircraft elements. Specifically excluded were standard portions of the RSRA airframe and standard S-61 flight hardware. These exclusions were allowed only after exhaustive comparisons and analyses confirmed similarity in terms of the physical hardware, its intended use, and anticipated operating environments. The exhaustive comparisons notwithstanding, cost and schedule penalties eventually were incurred as a result of this practice because of the inherent inability to determine, *a priori*, the effects of operational history. The primary basis for excluding S-61 hardware was the maturity of its reliability data and the acceptable trends of reliability demonstrated in service usage. An example of a reliability comparison analysis between the RSRA and the S-61 Presidential Airlift helicopter is shown in Figure 2.4-2. The exclusion of S-61 hardware constituted the first level of safety program implementation tailoring.

FMEA's were the first safety-related analyses performed. They are discussed in a safety context here because of their later application. These analyses were done by the contractor at the subsystem level and initial deliveries supported their respective PDR's. Subsequent updates and refinements supported the CDR's and system level reviews. When hardware schedule slips did occur (some reviews were accomplished incrementally), the FMEA schedules were adjusted accordingly. This resulted in no adverse effects, except for two major schedule adjustments that occurred, which required special safety engineering attention. These were the AIBS and the EES development, which slipped with the result that the systems were not operational until after the first flights. Special analyses and reviews were conducted and operational limitations imposed to allow flight without these systems. Schedule and cost penalties were controlled, and an acceptable level of safety was maintained.

A preliminary hazard analysis (PHA) was performed by the contractor after completion of the initial FMEA's. The purpose of performing the PHA at this time was to identify areas requiring additional safety effort prior to the flight readiness review (FRR) which occurred 6 months later. A Notification of Potential Hazard report resulting from that analysis is shown in Figure 3.1-3.



Sikorsky Aircraft — U A — REPORT NO.

RSRA SYSTEM SAFETY - NOTIFICATION OF POTENTIAL HAZARD

DATE: Jan. 7, 1976

HAZARD NOTE: E.24.24

FROM: J. Upton

TO: G. Chesley

CC: A. Linden, A. DeVoe, W. Fischer, P. Jeffery, R. MacLennan

POTENTIAL HAZARD: Main rotor series trim lateral cyclic actuator rod end bearing jammed due to lack of lubricant or contamination.

Category I = helo
Category II = compound

PROBABLE EFFECT:

Loss of control of rotary roll inputs.

RECOMMENDED ACTION:

Conduct proof test.

Define inspection interval.

ACTION TAKEN:

1) Design based on extensive previous experience.
2) Components designed to proof loads in excess of normal operational loads.
3) Subject to detection during preflight check.

ACTION APPROVED BY:

G. B. Chesley

PAGE

Figure 3.1-3 RSRA Preliminary Hazard Analysis Report

In retrospect, it probably would have been more project effective to perform the PHA earlier. This would have enabled better early definition of safety requirements and potential problem areas requiring greater safety emphasis. Ordinarily, system data of the detail indicated in Figure 3.1-3 are not available when a PHA is done.

A valuable lesson learned is that performing a PHA or top level fault tree early can focus attention on critical areas and identify the need for more comprehensive or specialized studies. Properly timed, PHA results are helpful in defining tools and their applications.

Detailed safety analyses had not yet been performed to the subsystem and system levels, nor had operational considerations been fully addressed. These analyses were required and were planned to support the FRR. Because the basic FMEA's had already been prepared and their further amplification was not needed, remaining allocated resources were diverted to the safety effort. In this case, the ability to meet research goals far outweighed the need to adhere to strict maintenance and flight schedules, considering the experimental nature of this project. Because of this, resources were reallocated from the reliability analyses to the safety effort. The FMEA's were amended to include a sheet "B" addressing safety issues, as shown in Figures 3.1-4 and -5 and thus became FMECA's. By adding "criticality," the hazards were addressed; by detailing the FMECA's to the subsystem level in addition to the system level, the system and subsystem levels of hazards were addressed.

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS - SHEET "A"

AIR VEHICLE RSRA
SYSTEM EFCS
ASSEMBLY SAS I AND SAS II
HYDRAULIC SHUTOFF VALVE

DESIGN D.R. Fowler DATE 3-27-76
SAFETY T.C. Burkhart DATE 3-27-76
HUMAN FACTORS Robert Fowell DATE 3-23-76

PREPARED BY R. o. Downing
DATE 3-16-76 PAGE 17 OF 29
REVISION NO. ______ DATE ______

Name and Identification No.	Quantity Per System	Function	Failure Mode	Failure Cause	Failure Effect On: System	Failure Effect On: Interfacing System	Failure Effect On: Air Vehicle
HYDRAULIC SHUTOFF VALVE			D. LOSS OF FLUID	D. LEAKAGE, LINE FRACTURE, HOUSING CRACK	D. EVENTUAL LOSS OF THE AFFECTED HYDRAULIC SYSTEM I OR II. LOSS OF SAS I OR SAS II.	D. IF HYDRAULIC SYSTEM I IS AFFECTED:	D. IF HYDRAULIC SYSTEM I IS AFFECTED:
						1. DETERIORATION OF ROTOR SYSTEM'S PRIMARY SERVO PERFORMANCE.	1. PRIMARY SERVO REDUNDANCY PROVIDED BY #2 SYSTEM.
						2. DETERIORATION OF ACTIVE ISOLATION SYSTEM PERFORMANCE.	2. ACTIVE ISOLATION SYSTEM LOCKS WILL ENGAGE WHEN PRESSURE DROP IS SENSED.
						3. LOSS OF EFFECTIVE REDUNDANCY TO HYDRAULIC SYSTEM #2.	3. NO DEGRADATION IN AIRCRAFT PERFORMANCE.
						4. LOSS OF REDUNDANCY TO PILOT BOOST SERVO, BACK-UP TRIM AND SAS III AND IV.	4. PILOT BOOST SERVO, BACK-UP TRIM AND SAS III AND IV REDUNDANCY PROVIDED BY HYDRAULIC SYSTEM NO. 3 HELICOPTER MODE AND BY HYDRAULIC SYSTEM NO. 4 COMPOUND (FIXED WING) MODE.
						5. LOSS OF REDUNDANCY TO ROTARY WING EFCS ACTUATORS.	5. EFCS ROTARY WING ACTUATOR REDUNDANCY PROVIDED BY HYDRAULIC SYSTEM NO. 2.

Figure 3.1-4 RSRA FMEA Example

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS - SHEET "B"

AIR VEHICLE: RSRA
System: [illegible]
Assembly: SAS I AND II (HYDRAULIC SHUTOFF VALVE)

DESIGN: D.W. Fowler DATE: 3-27-76
SAFETY: T.C. Burkhardt DATE: 3-27-76
HUMAN FACTORS: Robert [illegible] DATE: 3-27-76

PREPARED BY: R. O. Downey
DATE: 3-18-76 PAGE: 18 OF 29
REVISION NO. DATE

Name and Identification No.	Failure Mode	Failure Category	Possible Safety Hazard	Failure Detection Method	Operational Experience	Test Experience Failures	Test Experience Hours	Comments
HYDRAULIC SHUTOFF VALVE	A. COIL OPENS	III	NONE	A. AFFECTED SAS ON LAMP EXTINGUISHES				
	B. COIL SHORTS	III	NONE	B. SAME AS A				
	C. JAMMED OR BINDING SPOOL	III	NONE	C. INSPECTION, AIRCRAFT RESPONSE				
	D. LOSS OF FLUID	II	SEE AIR VEHICLE EFFECTS	D. COCKPIT INDICATION, INSPECTION				

Figure 3.1-5 RSRA FMECA Example

This was a second major tailoring of safety program implementation and, although not rigorously identical to system hazard analysis (SHA) and subsystem hazard analysis (SSHA), it at least served the essential purposes. The FMECA's were developed, reviewed, and appropriate implementation actions initiated through the combined efforts of system designers, safety engineers, and human factors personnel. The total FMECA, which generally fulfilled the purpose of the SSHA's and SHA's, was reviewed in-depth by all levels of contractor and Government project personnel. A hazard catalogue was produced to identify those issues requiring resolution prior to flight.

This approach focused the needed technical capabilities and resources on solving the real-world RSRA problems. It is an example of initiating the safety analysis activity in a single format and "maturing" it as the project progresses. Pitfalls in this approach are that, because of the detailed nature of the FMEA, system-to-system relationships may not be considered, and operating personnel and environment considerations may be overlooked. Great caution should be used in exercising this option. NHB 1700.1 (V3), Section 2, "Technical Methods," and MIL-STD-882A are excellent references for system safety tool application.

The FMECA's for the AIBS and EES were completed prior to the operational use of those systems, but subsequent to initial RSRA flight. They were prepared with the same rigor as the other analyses. Interaction with the previously analyzed systems was considered in formulating the final FMECA. This last step, relooking at work previously completed, was an essential step made necessary by the waterfall completion schedule.

Several other limited safety analyses were performed later in the project. Sneak Circuit Analysis of the EFCS planned early in the project was deleted in the interest of cost savings. It was performed much later after more costly alternate studies and tests were completed. The cost-safety trade (in favor of cost in this case) in retrospect, was not cost effective. In the words of the Project Manager, "Doing Sneaks early would have saved money (guess 10:1 payback) in fixing drawing errors. It also provides early identification of hazards or early confidence that they've been shaken out." Figure 3.1-6 shows one of the Sneak Circuit Reports delivered.

Other analyses performed late in the project included a top-level fault tree, Figure 3.1-7, a detailed EFCS fault tree, Figure 3.1-8, and an EFCS Common Cause Failure Analysis (CCFA), Figure 3.1-9.

PROJECT RSRA PAGE 1 OF 2

SNEAK CIRCUIT REPORT - 3

TITLE DUAL SERIES TRIM BEEP CONTROLS DO NOT PROVIDE THE SAME OUTPUT

REFERENCES

72401-01952	Rev. A	GRIP ASSY. CYCLIC
72404-01111	Basic	ACMU-EFCS/SAS/FFS
72404-01115	Rev. B	SERIES TRIM/EFCS
72404-01108	Rev. F	ACMU1

MODULE/EQUIPMENT - ACMU/XA7,XA8

EXPLANATION

The series trim control switches on the Safety Pilot and the Evaluation Pilot Grip assemblies are wired so that they will give opposite commands when energized in the left and right directions as shown in figure 1. When the SP Trim switch is energized left, No. 1 and No. 2 Actuators are commanded to extend; when the EP Trim switch is energized left, No. 1 and No. 2 actuators are commanded to retract. The opposing commands are reversed when the Trim switches are energized right.

POTENTIAL IMPACT

Permits conflictive commands to be issued to actuator which may damage actuator. Results in confusion when attempting series trim, may result in pilot issuing incorrect command.

RECOMMENDATION

Reverse the Extend and Retract wires going to the SP Series Trim Beep Switch.

REPORTED BY L. Urban DATE 1-15-80

CUSTOMER ACTION

BOEING AEROSPACE COMPANY HOUSTON, TEXAS

PAGE 2 OF 2

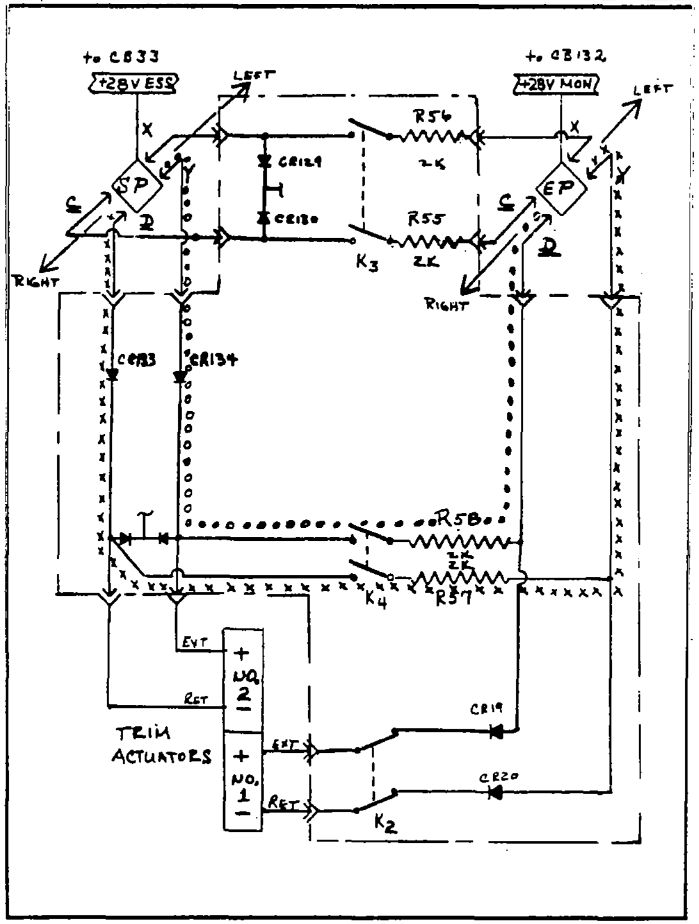


Figure 3.1-6 RSRA Sneak Circuit Example

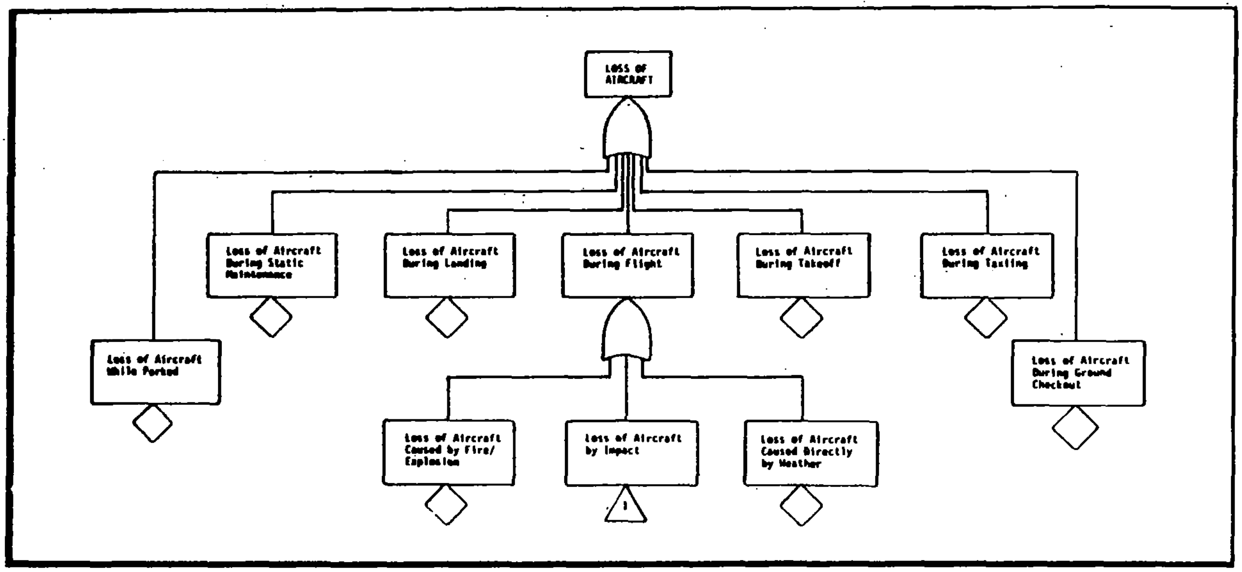


Figure 3.1-7 RSRA Fault Tree Analysis Example
(Top Level Fault Tree)

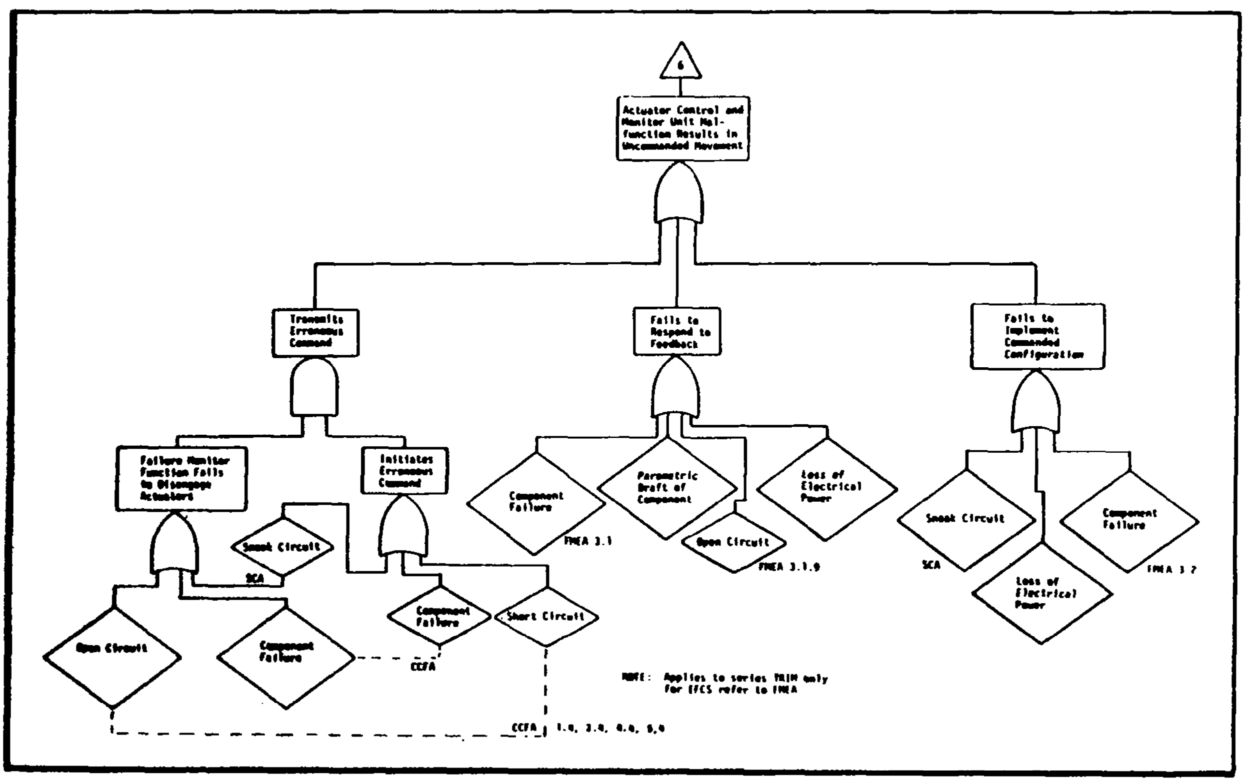


Figure 3.1-8 RSRA Fault Tree Analysis Example
(Detailed Fault Tree)

RSRA COMMON CAUSE FAILURE ANALYSIS

CRITICAL FUNCTION SET	COMMONALITY	CRITICAL EVENT	POTENTIAL CAUSE	EFFECT	REMARKS
1.1 ACMU AILERON POSITIONING A portion of the EFCS aileron control interface is provided by ACMU #1. Printed circuit card A6 provides for control of the two aileron EFCS actuators, while card A8 provides for control of the two aileron Series Trim actuators. A single event which causes loss of these outputs from both cards would result in inability to command aileron movement by the EFCS.	CONNECTOR XA8, ACMU #1 Pin 3 = PG1 Pin 4 = +15V S1 Pin 5 = -15V S1 Pin 6 = SG1 Pin 24 = AIL COMP IN #1 Pin 25 = AIL TRIM #1 ENG. SIG. Pin 29 = AIL TRIM #1 NO. 1 RATE SIG. Pin 30 = AIL COMP IN #2 Pin 31 = TO EFCS #1 Pin 32 = TO EFCS #2 Pin 33 = AIL TRIM #1 TRIM EXT. Pin 34 = AIL TRIM #1 TRIM RET. Pin 35 = EP STK TRM BP SW Pin 36 = EP STK TRM BP SW Pin 37 = EP STK TRM BP SW Pin 38 = EP STK TRM BP SW Pin 42 = SG4 Pin 43 = -15V S4 Pin 44 = +15V S4 Pin 45 = SG2 Pin 46 = -15V S2 Pin 47 = +15 S2 Pin 48 = PG2 Pin 52 = AIL TRIM #2 ENG. SIG. (Continued)	1. Pins 4, 44, and 47 open.	(a) Bent pins. (b) Corrosive/nonconductive contaminant. (c) Manufacturing defect. (d) Connector not mated.	Inability to command aileron movement by the EFCS.	Pilots may control ailerons using other flight control systems.
		2. Pins 5, 43, and 46 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1
		3. Pins 6, 42, and 45 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1
		4. Pins 4, 43, and 46 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1
		5. Pins 4, 42, and 45 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1
		6. Pins 5, 43, and 47 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1
		7. Pins 6, 42, and 47 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1
		8. Pins 5, 44, and 47 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1
		9. Pins 5, 42, and 45 open.	Same as 1.1.1	Same as 1.1.1	Same as 1.1.1

Figure 3.1-9 RSRA Common Cause Failure Analysis Example

These later analyses reflected the project manager's interest in ensuring that all areas had been addressed. The top-level fault tree identified the major areas of concern and subsequent review showed that all areas had been adequately covered in the FMECA and other studies.

The use of top-level fault tree analyses (FTA's), late in a project, is an effective tool for identifying problem areas overlooked or not properly addressed. Properly done, they can trigger a relook at previously completed analyses to verify their sufficiency.

The EFCS detailed fault tree and common cause failure analyses were accomplished in response to the project manager's concern that a third party review this safety critical area in which the project staff had the least expertise. While these analyses did not reveal any previously unidentified hazards, they served two very important purposes. First, they established confidence in the safety adequacy of the EFCS itself; second, they enhanced the credibility of the other system and subsystem analyses that had been performed.

In summary, project implementation in terms of techniques applied deviated from the plan. These deviations resulted from conscious decisions based on real-time needs and complied with the intent of the plan to produce a safe RSRA.

3.1.3 Assigning Review Authority and Methods. RSRA safety decisions were based upon informed positive actions. Risk was accepted, when necessary, by a conscious act, not through default. The project manager bore the ultimate responsibility for overall project safety, but he delegated authority for safety functions to his Chief Engineer. Review of safety matters was an integrated staff function, which was conducted at several levels throughout the organization. Activities ranged from the daily routine to rigorous formal committee action involving the Center Director. The subsystem managers reviewed the hazard analysis reports in-depth, working with detailed drawings, schematics, and other data. They consulted with staff technical personnel and outside experts when needed. They asked questions to establish credibility of the problem, investigated its potential impacts and concurred in appropriate resolution decisions. Those problems not immediately resolved were entered in the AQR and presented at major reviews (PDR, CDR, etc.). Resulting actions were reviewed by the Chief Engineer and approved by the Project Manager and the Aviation Safety Officer for all except safety-of-flight release, which required Center Director approval.

3.1.4 Providing Information Flow. The AQP specified the input and output data which flowed throughout the organization, between organizations and between the contractor and project office for the RSRA. Figure 3.1-10 provides a representative data flow leading up to Safety-of-Flight Release for the aircraft.

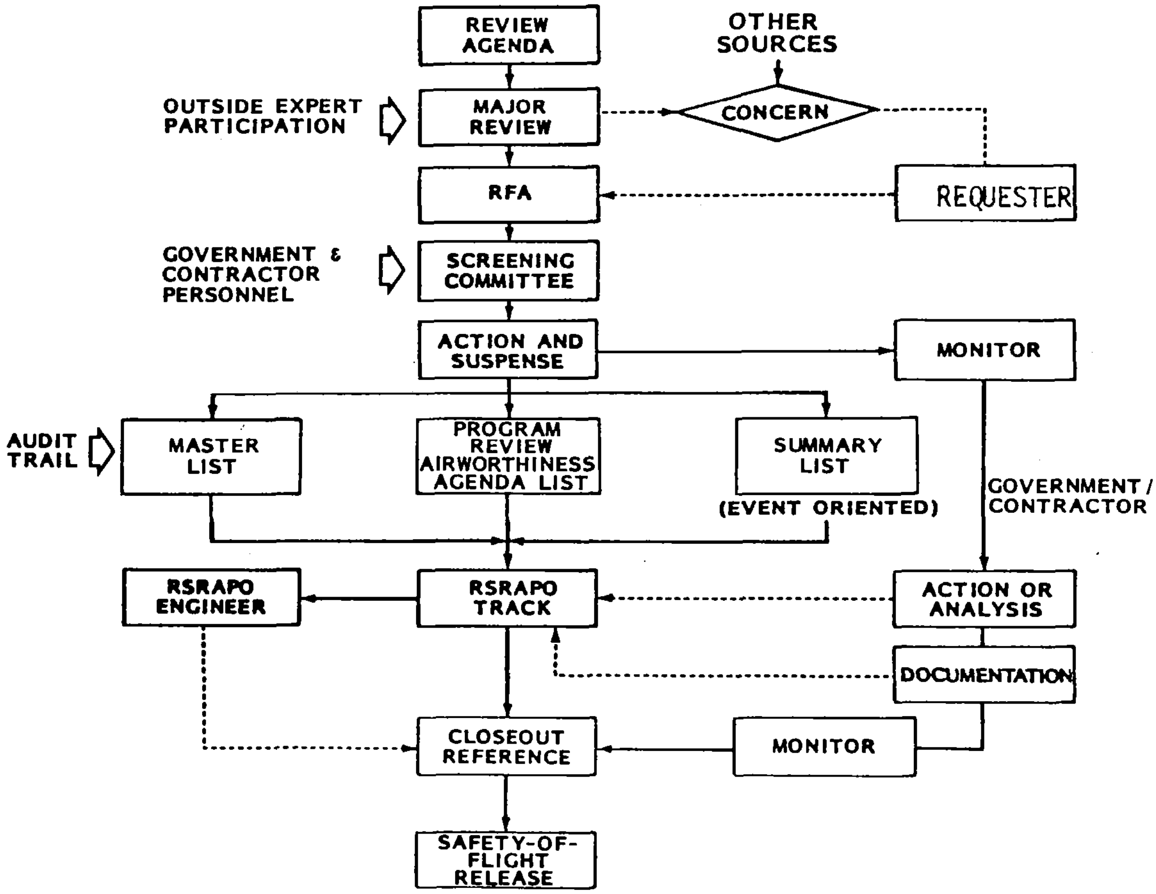


Figure 3.1-10 RSRA Concern Resolution Process

Formats, origins, and uses of information were described to guide project participants. In other words, after a hazard was perceived, the AQP described how it should be reported. It also addressed who should document the hazard and in what format. The AQP described where it went from there and who evaluated it. The plan covered how the evaluation was to be coordinated and recorded. It specified who was to be involved in resolution of the hazard and how that resolution would be implemented. Recording the implementation of the resolution was likewise specified in the AQP. Visibility provisions and documentation retention for reviews were also addressed. This systematic and disciplined approach established a documentation audit trail for closeout of identified risks and ensured that closeout actions did not occur on paper only.

Significant features of the AQR as reflected in the figure are: (1) Retention in the master listing of all concerns identified during the life of the project, their origins, and resolution actions required (this constituted an excellent audit trail and minimized unnecessary re-review of issues already put to bed); (2) use of the summary listing to provide a comprehensive index of all closeout documentation; and (3) concerns entered in the Program Review Airworthiness agenda list "tagged" for resolution by a specific major review.

The summary lists were a reordering of the master list and in effect established a prioritized ranking of concerns. Information on issues requiring resolution by or at the next milestone review was always readily available.

Those problems having the greatest programmatic impact were assigned to the "top ten." This group, not necessarily limited to ten, represented those issues which were potential "show stoppers." Representative problems (some of which are safety related, some simply programmatic problems) are shown in Figure 3.1-11.

1.	CALIBRATION FIXTURE EAC EXCEEDS BUDGET	- NOT FAILURE - PROGRAMMATIC ISSUE*
2.	AIBS DESIGN CONCEPT	- NOT FAILURE - PROGRAMMATIC ISSUE*
3.	FLIGHT TEST CONCEPT	- NOT FAILURE - PROGRAMMATIC ISSUE*
4.	DESCOPING	- NOT FAILURE - PROGRAMMATIC ISSUE*
5.	INADEQUATE PYRO. QUAL. SCHEDULES	- NOT FAILURE - PROGRAMMATIC ISSUE*
6.	BSA FAILS TEMP/HUMID CYCLING	- ITEM 2
7.	ANALYSIS INDICATES INTERFERENCE IN ESCAPE TRAJECTORIES	- ITEM 4
8.	APPARENT GROSS INACCURACY IN ROTOR LOAD MEASUREMENTS	- ITEM 3
9.	A1 BLADDER DEVELOPMENT AND QUALIFICATIONS	- ROUTINE DEVELOPMENT
10.	AIRCRAFT #2 INSTRUMENTATION INSTALLATION AND CHECKOUT SCHEDULE	- NOT FAILURE - PROGRAMMATIC ISSUE*
11.	WING TILT ACTUATORS DID NOT OPERATE IN HARMONY	- ITEM 8
12.	ACCUMULATOR THREAD FAILURE DURING PROOF PRESSURE TESTS	- ROUTINE DEVELOPMENT
13.	A1 BLADDER QUALIFICATION (AGAIN)	- ROUTINE DEVELOPMENT
14.	A1 DAMPER NULL PRESSURE SENSITIVITY TO TEMPERATURE	- DESCOPED
15.	SAS AND SERIES TRIM ACTUATOR PROCUREMENT/ QUALIFICATION	- ROUTINE DEVELOPMENT
16.	LATE COMPLETION OF SEAT DESIGN, DEVELOPMENT AND QUALIFICATION	- ITEM 5
17.	UNRESOLVED CRITICAL FAILURE MODES	- NOT FAILURE - PROGRAMMATIC ISSUE*

* COST PROBLEMS REQUIRED DESCOPING

Figure 3.1-11 RSRAPO Program Development Problems - Top Ten

The status of the top ten problems and the actions to assure their resolution were regularly presented for NASA Center management review. This technique was a very effective method of prioritizing project efforts. In the words of the RSRA project manager, "When you tell upper management what your potential show-stopper problems are, you can be sure you get their attention, their guidance, and their help (possibly even more than you think you need!)."

This focused attention might lead to fear of an overkill on problem resolution. RSRA experience indicated that such extraordinary effort on project-critical problems was appropriate. The process of identifying, assessing, and resolving concerns identified at reviews, together with the detailed documentation procedure, serves as an example for future programs. Well planned and timed reviews and thorough, traceable documentation were major factors in the success of the RSRA project.

3.2 ORGANIZING THE PEOPLE. Special inter- and intra-organizational relationships were established in the formation of the RSRA project team. Safety task requirements and organizational responsibilities were imposed by the AQP:

> Flight Readiness Review. - Conducted two months prior to first flight of each air vehicle configuration (helicopter, compound, fixed wing, and with active isolator). Chaired by the Center Aviation Safety Officer (ASO). Contractor WBS Managers for Design, Test, and Systems Engineering will substantiate the airworthiness and safety-of-flight release, the flight development buildup plan, safety-of-flight provisions, and emergency procedures. Review Chairman, assisted by Secretary, will identify open action items and will submit report of determinations and recommendations to the Project Manager.
>
> Pre-Flight Reviews. - Conducted just prior to first flight of each air vehicle configuration. Chaired by the Aviation Safety Officer. Open items from FRR are reviewed to confirm acceptable resolution. Review chairman will verify that airworthiness and safety requirements have been satisfactorily achieved, and will report determinations and findings, including recommendations for safety-of-flight release for approval by the Director.
>
> Review Action. - Government responsibility to participate in reviews as specified in NASA/Army Project Directive Number 1. Government or contractor review team members shall use the Request for Action (RFA) form to identify any elements of noncompliance with specifications, with program requirements or with program objectives as they affect airworthiness, safety, or Reliability and Quality Assurance (R&QA). RFA action assignees will incorporate action items in the AQR, and will review corrective actions and verify resolution. Responsibility - Review Team Chairman to assign action by RFA and provide report of review determinations and recommendations.

The authority to implement those requirements was delegated to the NASA RSRA Project Chief Engineer. The resulting organization was designed to optimize the flow of information and maximize the benefit to be derived from available skills and training. Additionally, the organizational structure paralleled the contractor's to balance the interfaces and facilitate coordination.

NHB 1700.1 (V3),"System Safety," contains the following statement relative to the safety function and its place in the organizational structure.

> . . . it should be placed in the reporting chain at a point which allows the risk evaluation output resulting from the safety effort to flow directly to the appropriate level of management in support of risk management decisions.

The RSRA safety function was implemented through the Project Chief Engineer, who had direct access to the project manager, the Aviation Safety Officer, and the Center Director. He had sufficient authority to implement safety requirements and appropriate problem resolution measures.

Although only one NASA employee carried the "safety" label, it was not a one-man show. The functional safety effort complied with NHB 1700.1 (V3), which states:

> The organization of the functional system safety effort is developed to accomplish the tasks set forth in the safety plan. Safety may be part of the system engineering organization or part of a systems effectiveness organization, collocated with the reliability, quality or maintainability organizations. As a general rule, to maintain objectivity and the check and balance system, it is preferable that system safety not be part of the design engineering organization.

The RSRA Project Chief Engineer was also the System Engineer Manager, and the System Safety and R&QA managers reported to him. Tailoring safety requirements to the project in terms of organization involved collocating the safety engineer with the systems engineering organization, and the sharing of safety responsibilities by all WBS managers. The RSRA experience shows that this arrangement <u>can</u> be effective; however, it also raises a question: Would this arrangement be as effective on other projects or should its success be attributed more to the safety attitude and competence of the RSRA staff?

The NASA focal point for safety matters was the project safety engineer, whose authority was through the Chief Engineer. A safety counterpart was designated in the contractor's shop and close coordination was maintained between the two. These individuals were the focal points in their respective organizations; however, they did not have sole responsibility for RSRA safety. Other in-place NASA elements were employed on a consultation basis, or as sounding boards when conditions merited. The RSRA staff was involved in each level of project safety activity. The organizational concept that each Work Breakdown Structure (WBS) manager was actually a miniproject manager was significant. Each of these managers was responsible for technical performance, cost, schedule, safety, reliability, and other facets of his WBS element. By involving the project organization in developing the plan, each WBS manager had to address what he would do to support project safety. Thus management on the RSRA project was knowledgeable concerning system safety and was keenly aware of safety as an integral component of project success. This safety-conscious attitude pervaded the organization and resulted in a continuous team effort to include safety in mainstream project activities.

An important lesson learned is that by organizing for safety, the experience of other staff members and in-place organizations can be used effectively to augment even an austere safety program.

3.2.1 Providing Required Information

The success of the RSRA project in general and the safety program in particular, depended upon acquisition, generation, and dissemination of information. This included information generated by the contractor as well as the project office. The most effective organization for accomplishing this was one consistent with the contractor organization. Accountability for safety resided with each director as described in NHB 1700.1 (V1). Accountability was further distributed to project managers together with the required authority. The structure for safety accountability and authority within the RSRA project was documented in the AQP. The organization for safety is illustrated in Figure 3.2-1.

The organization provided for subsystem responsibility as well as technical discipline responsibilities not limited to a specific subsystem. An important feature was the establishment of a safety focal point. Participation of all staff members in safety activities provided comprehensive safety capability through coordination by the focal point.

The RSRA project office used the classic NASA concept of penetrating the contractor's activities in detail. The data clause in the contract gave the Government access to all contractor internal documentation related to the contract. Similar penetration of subcontractor activities was provided and pursued. One problem in this area resulted from the Emergency Escape System (EES) contractor's insistence on a firm fixed price contract with a proprietary rights provision. This contractual arrangement resulted in considerable difficulty in obtaining the information required for the necessary hazard analyses. The problem was overcome only by developing a close professional relationship between the Government and the subcontractor.

3.2.2 Using Skills and Training. The broad range of disciplines spanned by the safety tasks dictated the use of many skills. The entire project organization was, in fact, available to support the safety function. Safety concepts and techniques were essential to meeting the safety criteria, but a large staff of safety engineers was not considered necessary. In fact, only one project office person had "safety" in his title, and he also handled other system engineering disciplines (aerodynamic performance and mass properties). The project team itself was safety conscious and possessed the requisite system technology as well as technical design and development engineering skills. A single safety engineer, operating through the Chief Engineer, spearheaded RSRA safety activities. Safety consciousness of the project was fostered by safety seminars, coordination of safety activities, and, most importantly, by the project manager's positive attitude. Unique

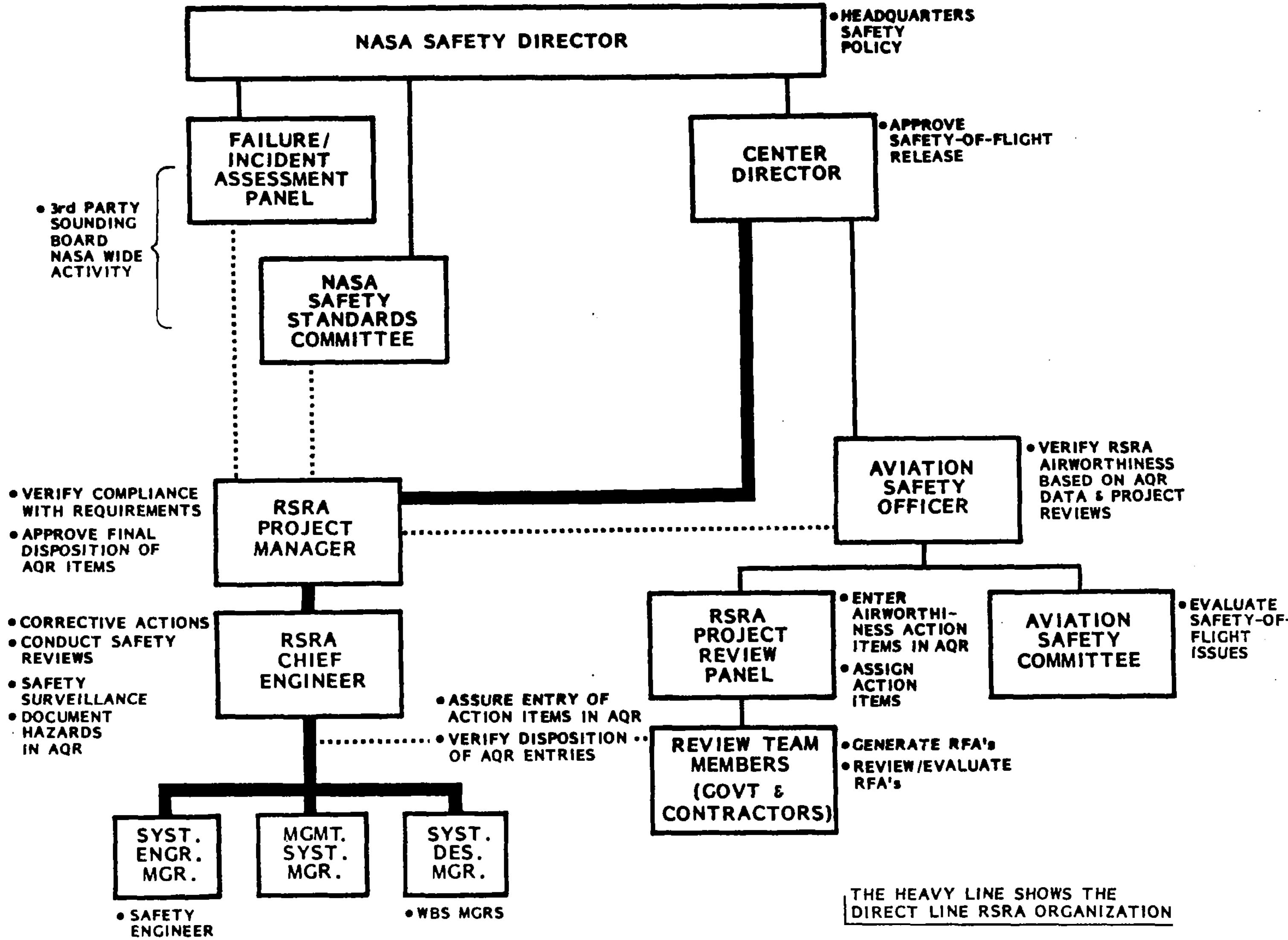


Figure 3.2-1 RSRA Safety Accountability Structure

capabilities of individuals played a significant role. As an example, both Government and contractor flightcrews and flight test engineering teams performed simulations and chalk-talk walkthroughs of stability and performance envelopes, normal operating procedures, and emergency procedures. They participated in pre- and postflight briefings and data reviews. Investigation of the cockpit layout by a flight crewmember in the design phase identified a control which operated opposite to the pilot's natural reaction. The design was changed to accommodate the natural reaction. Such perspective added a dimension normally unavailable, even in large safety organizations.

A lesson learned is that a very small safety staff can be effective if proper management support is provided. Don't try to out-engineer the experts. Technical quality of the safety product is enhanced when a safety expert guides the development of safety analyses through the knowledge of designers and system specialists. Assistance from sources external to the project was actively sought and encouraged. Senior people in diverse fields supported scheduled reviews. Since they weren't connected with the program, they had different perspectives and provided insight not normally available. A roster of participants in such RSRA safety reviews is shown in Figure 3.2-2.

DATE	REVIEWS	TYPICAL PARTICIPATION
NOV. 11, 1974	PDR	PRIME CONTRACTOR (SIKORSKY)
FEB. 6, 1975	DESIGN REVIEW	SUBCONTRACTORS (STANLEY, TMS)
JUNE 5, 1975	AFT FACING SEAT TECH. REVIEW	CONSULTANTS (McD/DAC, GRUMMAN)
JUNE 9, 1975	CDR	RSRA PROJECT OFFICE
NOV. 7, 1975	DEVELOPMENT STATUS REVIEW	LaRC, SED, RS&QA
JAN. 30, 1976	DEVELOPMENT STATUS REVIEW	AMRDL
FEB. 11, 1976	DEVELOPMENT STATUS REVIEW	AFSC HAFB TEST TRACK
AUG. 10, 1976	FINAL CDR (TEST READINESS)	AFSC/ASC B-1 (OSCAR SEPP)
APR. 14, 1977	TEST RESULTS REVIEW	USAF McCAFB (DAVE KETCHESON)
JUNE 16, 1977	QUALIFICATION REVIEW	NASC (FRED QUILL)
		USAMC (COL. DR. W. SCHANE)
		JPL (NAT. PRESCOTT)
		JSC (THOMAS GRAVES)
		DFRC (BRUCE PETERSON)
		USAF KAFB B-52 (ELLIS SMITH)

Figure 3.2-2 NASA/Army Rotor Systems Research Aircraft Project Safety Review Briefing, EES Review Participation

3.2.3 Avoiding Cultist Attitudes. The potential for "cult" development was recognized by the RSRA project manager. Through close coordination and personal involvement in the project, he maintained a balance between the needs of the project and the "wants" of individual discipline practitioners. Even though this project was relatively small, there was the risk of technical specialists (e.g., safety, R&M, weight and balance) wanting to stress compliance with their specialty disciplines at the expense of more essential work. When the Chief Engineer uncovered an unanticipated fatigue strength uncertainty, he "horse-traded" manhours from some of the "ility" effort to the more critical fatigue analysis. The tradeoff, which redirected scarce resources from lower priority mission availability analysis effort to accomplishment of essential safety studies, is a classic example of acute management awareness of the "cult" problem.

3.2.4 Balancing Contractor Interfaces. The organization of the RSRA project office paralleled that of the contractor's project. This resulted in a one-on-one working relationship at the subsystem level. This arrangement resulted in a cooperative working relationship providing mutual benefit, once the Government team had "earned their spurs" by convincing the contractor engineers of their technical competence and set aside fears of Government spying.

At least one case existed on the project where a member of the project office displayed deficiency in both performance and in interfacing effectively with the contractor. The project manager chose the difficult solution of prohibiting that person from traveling to the contractor's plant and, eventually, forcing his transfer out of the project without replacement. This required combining efforts by the project manager and other project personnel to fill the void.

While close technical cooperation between Government and contractor personnel was essential, it was the responsibility of NASA project management to ensure the highest reasonable quality of product consistent with cost and schedule constraints. It was at times necessary to adopt a "show-me" attitude. This adversary relationship is best illustrated by the one-on-one review of the contractor produced FMECA's. The contractor was frequently challenged to provide rationale for his classification of hazards, or substantiate supporting data. It was a fine line to be walked, and not always successful, as related above.

3.2.5 Facilitating Coordination. Most aspects of the coordination that occurred during the RSRA project are discussed elsewhere in this document. However, problems associated with the contractor's remoteness of location from the NASA project office deserves special attention. A discussion of the relocation of the project offices and flight test operations from Langley to Ames is provided in a later section. Real-time communications between the East Coast contractor facility and the West Coast Government facilities were burdensome at best. Extended Government and contractor personnel travel was required, and less person-to-person communication occurred. Successful project performance was achieved, but only through personal dedication, much added cost, and considerable personal inconvenience.

3.2.6 Cultivating an Ombudsman. Differing professional opinions are not uncommon. When this occurs, suppression of concerns sometimes results, especially in the case of disagreements between people related vertically in an organization chart. This problem was circumvented on the RSRA project with an ombudsman -- a person to hear the concerns of others on an unbiased basis.

An individual emerged from within the project to fulfill this function. Although his primary duties were not safety, his work was closely related to safety; he was perceptive; he had high integrity and tact; and he was interested. On many occasions he acted as a go-between to get things done informally, which may never have been accomplished through the formal route. Through this medium of communication, problem causes were isolated without fear of "punishment." Liaison was augmented and corrective actions and project improvements implemented.

The "lesson learned" is to be sensitive to, and encourage, the emergence of such informal channels of communication.

4.0 DIRECTING

Risk Management applied to the RSRA involved the process of identifying risks, reducing them, controlling those that couldn't be reduced, making conscious (not by default or ignorance) decisions to accept risks, and the discipline to make all of the above happen and to track the resolutions. This section addresses the elements of direction necessary to achieve effective project risk management.

4.1 ASSIGNING SAFETY ACCOUNTABILITY AND AUTHORITY

Specific RSRA accountabilities, provided for in the AQP, are illustrated in Figure 4.1-1.

TABLE I. - AIRWORTHINESS QUALIFICATION REVIEW ITEMS

STATUS THROUGH January 15, 1978

WBS	Contract Data Item Supplement III	ITEM	RSRA RESPONSIBILITY	DUE DATE	NOTES:	
System Safety & Reliability	1C 60 DA PDR	Hazard Catalogue	Systems Engineering	9/16/74	X SER72012	9/9/74
	1C 60 DA CDR	Hazard Cat., Rev. 1	Systems Engineering	8/11/75	X SER72012	7/24/75
	1C 90 DB PFR	Hazard Cat., Rev. 2	Systems Engineering	6/7/76	X PML 76-358	7/8/76
	1C 30 DB PFR	Hazard Cat., Rev. 3	Systems Engineering	8/7/76	X PML 76-358	7/8/76
	1A PFR	Preflight Safety Rept.	Systems Engineering	9/7/76	X FRR Rept. & PFR AQR Appendix A	7/8/76
	1B	Accident Report	Systems Engineering	As required	N/A	
	1D	Hazard Notification Sheet	Systems Engineering	As required	N/A	
	23 15DB CDR	FMEA's except AI & EES	Systems Engineering	12/27/75	X CDR Rept.	6/1/76
	23 15DB CDR	FMEA/AI	Systems Engineering	6/30/77	X SER Due	1/30/78
	23 15DB EES Qual.Rev.	FMEA/EES	Systems Engineering	4/30/77	X RSRA 1149	7/13/77
	23 15DB Comp. FRR	FMEA/Comp. + EFCS	Systems Engineering	4/30/77	X FRR Report	7/29/77
	23 Delivery	FMEA Final Revision	Systems Engineering	9/30/78		
	19	Failure Reports	Systems Engineering	As required	N/A	
Design Data/ Documentation	2 10 DB PDR	Perf. Stability Control Rept.	Systems Engineering	6/9/74	X SER72006	6/21/74
	2 330 DA PDR	Perf. Stability/ Cont. Rept., Rev. 1	Systems Engineering	5/16/75	X SER72006	3/18/76
	2B 100B PDR	Flt. Cont. Sys. Design Report	WBS Manager	6/25/74	X SER72007	6/20/74
	3 100B PDR	Structural Criteria	Systems Engineering	6/29/74	X SER72005	6/20/74
		Weights Report			X SER72004	4/30/74

Figure 4.1-1 RSRA Safety Accountability Assignments

RSRA project management recognized that the manner in which assignments and authority were distributed throughout the organization was important. If the majority of the safety issues were the responsibility of the most junior engineer on the project, and he alone was held accountable, the value assigned to safety would be obvious, and the product would be less than optimum. Every member of the staff, from the chief engineer to the junior engineer, had a definite role in ensuring safety. The subsystem managers were keenly aware of cost and schedule impacts of their subsystems on the overall project since they were held accountable for these items. The RSRA risk posture was enhanced when these managers were also held accountable for safety, as illustrated in Figure 4.1-1. To discharge this added responsibility, the RSRA subsystem managers developed a productive and close working relationship with their contractor counterparts. For example, the FMEA results prepared by the contractor were reviewed in detail by the subsystem managers and their technical people, to fully explore the impacts of identified failure modes.

4.2 FOSTERING SAFETY ATTITUDES. Safety awareness was part of daily project activity. An atmosphere of openness among staff members permitted discussion of the cost of performing each safety task. Schedule slips were freely discussed at all levels. No one liked added costs or schedule slips, but if staff members had failed to address these subjects, many safety problems may have been temporarily suppressed only to surface later.

The RSRA project manager's attitude was instrumental in the success of the project safety program. He was willing to consider opportunities, and was consistent in his willingness. He conveyed to his staff his willingness to consider every safety concern identified, when it was identified. He believed that safety tasks were finite, identifiable, definable, and do-able, and that if the tasks were competently done they would reduce accidents. In short, he believed that safety contributed to the betterment of the project, and was not just extra work. He conveyed to his staff his conviction that safety was important.

Cartoons and other types of humor were not uncommon during the course of the RSRA project. They were a subtle reminder of the need for safety awareness. The project manager didn't encourage humor -- he just let it happen. Humor, whether in cartoons or other forms, is a method of communication. The attitude of the staff and their concerns about the project were often conveyed in this way.

4.3 ENSURING INTERFACES. Communication was key to directing all aspects of the project. It was especially crucial in safety areas. One of the most common and most useful methods of communication was the staff meeting. The staff meeting provided the opportunity to convey matters of safety to those most closely associated with the project. It also cut across organizational boundaries and involved everyone in safety issues.

Significant, but less formal communications occurred daily in the development process. In RSRA, as in any development project, numerous conversations occurred between the Government project manager and the contractor project manager. Impromptu meetings, telephone calls, etc., were essential to getting the job done. It is probable that more progress was made through this type of communication than through the more formal meetings and reviews. Major agreements or decisions made in informal communications were documented. RSRA project management was very successful in establishing informal two-way communication with contractor technical personnel while at the same time observing the "arm's length" philosophy. This was, in fact, the communication mechanism through which resolution of the RSRA fatigue substantiation problem discussed in Section 5.3 was brought about.

4.4 RESOLVING HAZARDS. Hazard identification tools, information flow for transfer of technical data, and milestone review participation were described in earlier sections. These activities, in concert, yielded a shopping list of safety issues requiring evaluation and resolution.

Hazard resolution activities, specified in the AQP, were assigned to staff personnel at the working level, were formalized through major review activities and were documented in the AQR. The techniques applied were largely the same whether resolution was accomplished within the project, through the assistance of outside panels and committees, or by review board directed activity.

Hazard evalution and resolution techniques were not defined in the AQP; therefore, RSRA project management planned for and implemented a systematic approach similar to that outlined in MIL-STD-882A, described in the paragraphs below:

> When hazards are not eliminated during early design, a risk assessment procedure based upon the hazard probability as well as hazard severity, may be required to establish priorities for corrective action and resolution of identified hazards.
>
> Hazard severity categories are defined to provide a qualitative measure of the worst potential consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure or malfunction . . . .
>
> The probability that a hazard will occur during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity . . . . A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems.

Hazard categories I through IV as discussed in Section 2.4.1, were used to determine severity. Use of this technique and subsequent elimination or control of categories I and II hazards were imposed as requirements.

Rigorous quantitative evaluations of probability were employed only where precise, pertinent data were readily available or could be derived and where a real need existed for such precision, as in determination of rotor shaft safe life. Qualitative evaluations determined whether the hazard was likely or unlikely to result in an accident or unplanned event during the useful life of the aircraft. An example taken from RSRA experience was the inadvertent actuation of the EES seat barostat during installation. Evaluation determined that the event was a "one time" failure that could not be isolated to a cause. Corrective actions were, however, taken to resolve all of several postulated causes, even though the consequences of the actuation were not likely to be critical. This over response approach is not uncommon where pyrotechnic devices are involved.

The approach for hazard resolution was also based upon MIL-STD-882A:

> Action shall be taken to eliminate or minimize hazards revealed by analyses or related engineering efforts. Catastrophic and critical hazards shall be eliminated or controlled. If these hazards cannot be eliminated or controlled to an acceptable level, the alternative controls and recommendations will be immediately presented to the managing activity.

When an identified hazard impacted safety criteria satisfaction, resolution was accomplished in accordance with the Hazard Reduction Precedence Sequence.

a. Design for minimum hazard.

b. Employ safety devices.

c. Employ warning devices.

d. Implement procedures and training.

The above sequence of hazard reduction methods is given in descending order of safety priority; but, again, the choice was made within the objectives of the project as a management trade consistent with resource and performance goals. Safety was compromised "vertically" in the sequence only as performance or resource limitations dictated. Full evaluation of each option of the reduction sequence sometimes resulted in a decision to accept the risk.

Throughout the process, the RSRA project manager maintained the required balance among performance, resources, and safety factors. He applied the Hazard Reduction Precedence Sequence while maintaining a clear view of the requirements to be satisfied. If the hazard could be eliminated through design, while maintaining the balance among the three controlling factors, the design change was implemented. Category I hazards that could not be eliminated through design required the application of the "safe life" concept. The design of the main rotor shaft provides an example. Statistically representative samples were tested to predict the safe useful life of the shafts based on the concept that catastrophic failure modes existed and had finite probabilities. The predicted useful life was derated, and maintenance and inspection intervals were specified to ensure changeout before critical failure could occur. Another example of this concept, where "safe life" was less predictable, was the development of the contractor's (Sikorsky) Blade Inspection Method (BIM)®. This technique allowed pressurization of the rotor blade spars and detection of any subsequent loss of pressure which would be indicative of incipient catastrophic structural failure. This precaution enabled acceptance of an unavoidable single point failure condition.

Category II hazards which could not be eliminated through design were controlled through the use of redundancy. Design of the main rotor load measurement system, through which the main rotor and transmission are connected to the fuselage, is an example. Measurement system accuracy requirements could best be achieved by the use of three load cells. However, safety considerations dictated the use of as many load cells as possible to preclude structural failure. Each additional load cell (beyond three) decreased measurement accuracy and fewer load cells decreased safety. The final design employed four load cells resulting in fail-safe measurement system design, satisfying both performance and safety requirements.

In some cases, fail-safe design was not sufficient. Such a situation arose on the RSRA project when a stability problem required operation of the Stability Augmentation System (SAS) to ensure safety. Because of its criticality, it was apparent that a very detailed reliability analysis was needed. Unfortunately, the contractor was not required to perform this type of analysis and the Government team lacked the required staff. On the plus side, a qualified analyst, engaged in another program, was available for the short time necessary to accomplish the study, and another "horse trade" got the job done. The analysis concluded that the SAS design had to be dual redundant, to tolerate two failures and still be operational (fail-op/fail-op). The addition of the SAS redundancy greatly impacted cost, but the required degree of safety could not be obtained without it.

Although many hazards can be resolved through design changes, those solutions must be evaluated in terms of performance and resource cost. This evaluation may drive the solution lower in the Hazard Reduction Precedence Sequence scale or direct the acceptance of some risk. The RSRA escape system provides an illustration. Ejection at the higher flight envelope speeds was found to be clearly unsafe. The evaluation revealed an unacceptable potential for loss of life of the flightcrew. The resolution decision weighed whether or not to extensively delay the program and overrun costs while the escape system was redesigned. Both performance and resources would be severely impacted by proposed redesigns. No feasible way of erecting barriers around the crew or raising their damage thresholds was conceived. Qualification testing had demonstrated that the emergency escape envelope was less than the aircraft flight envelope. However, precedent for this problem had been established on the F-111 program.

RSRA project management carried the issue to a third party "jury" of experts shown in Figure 3.2-2. The decision was made to accept the situation under specific conditions. First, only limited operation would be allowed beyond the safe ejection envelope. Second, a preflight briefing would be held to heighten hazard awareness whenever the escape envelope was to be exceeded. Third, the preflight briefing would include a review of the proper recovery procedures; i.e., return to the "safe" envelope. Fourth, recovery procedure training would be accomplished through simulation to ensure proper pilot reaction (it was a natural response). The hazard remained, but its LIKELIHOOD was minimized by controlling the flight envelope. During limited excursions beyond the safe operating boundary, WARNING, TRAINING, and ESCAPE were counted upon. The risk was identified and evaluated, and a mutually acceptable resolution implemented.

These experiences from the RSRA project demonstrate that problems encountered in an aircraft development program can be resolved through sound management practices. As a final note, it is sometimes impossible to avoid risks and still retain a viable project. Incorporation of the previously discussed EES is just such an example. The EES serves no useful project function, other than to save the crew if a catastrophic event should occur. It exists only because the project exists and includes, as does any flight project, certain risks.

For future programs it would be valuable to have a systematic/disciplined approach to hazard evaluation and resolution either outlined or referenced in the plan. NHB 1700.1 (V3), System Safety, and MIL-STD-882A, Military Standard System Safety Program Requirements, are excellent references.

5.0 CONTROLLING. The RSRA project control activities were used primarily to verify compliance with the plan and were in essence an ongoing audit. Variances from the plan did occur. Some were anticipated, some were not. All were responded to and subsequent planning was adjusted accordingly.

5.1 CHECKING PROGRESS. Controlling the safety aspects of the RSRA project was a matter of maintaining an awareness of current status and taking appropriate action. The schedule established in the AQP identified periodic reviews for assessment of progress. These reviews (except for the obvious safety implications of the FRR) were rarely separate safety reviews. As in every project, reviews were scheduled -- PDR's, CDR's, FRR's, etc. By the addition of safety as a standard agenda item, performance, resources, and safety status of all elements were assessed interactively at the same meeting. Data flow associated with a typical RSRA project milestone review was shown in Figure 3.1-10. Safety activities were integrated into the mainstream of RSRA project development by their inclusion as agenda items in formal reviews, as illustrated in Figure 5.1-1.

1. RESEARCH CAPABILITY (SEE FIGURE 3)
2. SYSTEM/SUBSYSTEM DEFINITION
3. PERFORMANCE REQUIREMENTS
4. LOADS/STRENGTH
5. MATERIALS, PARTS, PROCESSES
6. INTERFACE (INTEGRATION) REQUIREMENTS
7. SAFETY
8. RELIABILITY/MAINTAINABILITY
9. HUMAN FACTORS
10. QUALITY ASSURANCE PROVISIONS
    - AIRWORTHINESS QUALIFICATION REQUIREMENTS
    - DESIGN ANALYSIS REQUIREMENTS
    - INSPECTION REQUIREMENTS
    - TEST AND MEASUREMENT REQUIREMENTS AND PLANS
12. DRAWING RELEASE SCHEDULE (INCLUDING SUBCONTRACTOR), RELATED TO PROCUREMENT/FABRICATION PLANS
13. RESOURCES:
    - COST/SCHEDULE STATUS AND PROJECTIONS (BCWS, BCWP, ACWP, CVAR, EAC)
    - BASIC DATA ENGINEERING HOURS (BCWP, BCWS, ACWP, SVAR, CVAR)
    - REASONS FOR C/SVAR, PROJECTED IMPACT, WORK-AROUND PLANS
    - STATUS OF POST-PRELIMINARY DESIGN WORK
    - PROCUREMENT STATUS AND PLANS
14. SCREEN AND ASSIGN ACTION ITEMS

Figure 5.1-1 Typical RSRA Review Agenda

In addition to the design and flight readiness reviews, RSRA project safety reviews were conducted when special safety emphasis was required. These were reviews of the hazard analysis methods and results, as well as the resolution of identified hazards. Examples of items considered at these reviews are shown in Figures 5.1-2 and 5.1-3.

NASA/ARMY ROTOR SYSTEMS RESEARCH AIRCRAFT (RSRA)

SAFETY REVIEW BRIEFING

I - DESIGN , (C) HAZARD ANALYSES-FMEA-CRITICAL ITEM CONTROL

CRITICAL ITEMS IDENTIFIED BY HA/FMEA, DESIGN/TEST REVIEWS, FLIGHT SAFETY REVIEWS, ETC.

- SCOPE OF HA/FMEA TAILORED (FLIGHT CONTROLS, LOAD CELLS, AIBS, EES) (60 SUMMARY ITEMS)
- OVERBEY SAFETY REVIEW PLAN (400 ITEMS) (47)
- EXTRA-ORDINARY SAFETY RELIABILITY ANALYSIS OF (FAIL OP)^2 SAS
- EFCS SNEAK CIRCUIT ANALYSIS NOT IMPLEMENTED (COST AVOIDANCE)

Figure 5.1-2 RSRA Hazard Analysis Results Review Example

NASA/ARMY ROTOR SYSTEMS RESEARCH AIRCRAFT (RSRA)
SAFETY REVIEW BRIEFING

HAZARD ANALYSES-FMEA-CRITICAL ITEM CONTROL

- EVERY CAT I OR II FAILURE MODE RESOLVED (49)
  - DESIGN CHANGE TO DOWNGRADE CRITICALITY
  - ANALYSIS/TEST TO VERIFY REMOTE PROBABILITY (SAFE LIFE)
  - INSPECTION REQUIREMENT TO DETECT (FAIL SAFE)
  - PREFLIGHT PROCEDURES TO VERIFY INTEGRITY
  - CAUTION/WARNING PROVISIONS AND EMERGENCY PROCEDURES TO CONTROL
  - CRITICAL COMPONENTS SERIALIZED AND TRACKED IN A/C LOG
  - CUMULATIVE FATIGUE DAMAGE TRACKED FOR EVERY E_W EXCEEDANCE
  - OPERATIONS GROUND/FLIGHT CREW AND TEST TEAM FAMILIARIZED DURING DEVELOPMENT
  - DOCUMENTATION WILL PASS WITH AIRCRAFT TO OPERATIONS TEAM

Figure 5.1-3 RSRA Hazard Resolution Review Example

Reviews of this type enabled RSRA project management to redirect the safety efforts when required. The redirection of the FMEA efforts toward FMECA's resulted from this type of review. While formal reviews were excellent places to measure progress, everything was not left until the next formal review. An open door policy was maintained to resolve difficulties before they grew into major problems. Impromptu meetings were called when problems arose. Independent inspection teams provided valuable checkpoints on project safety.

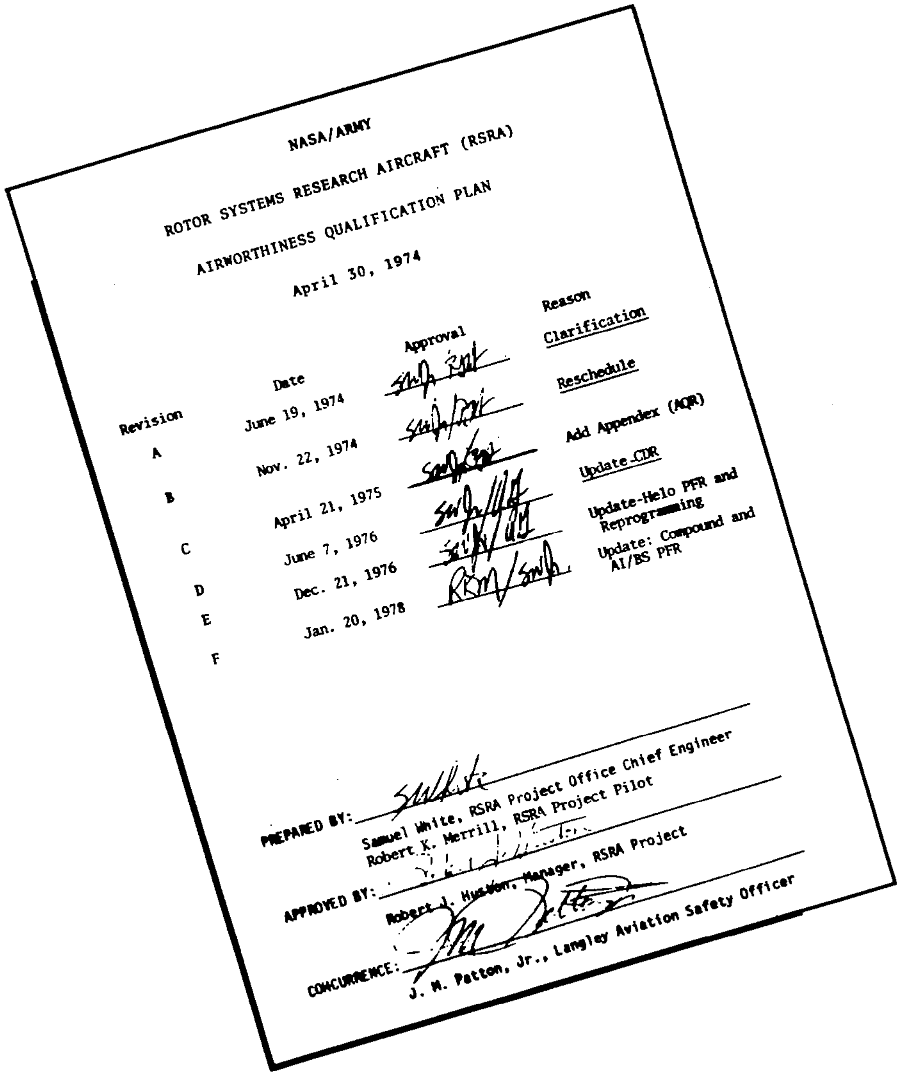
The preflight safety inspection of the RSRA provides an illustration. The contractor completed the preflight safety inspection, primarily by certified Quality Control inspectors, who were properly concerned with conformance of the hardware to drawings and to safety practices such as safety wiring of connectors. The Government safety inspection team, without reference to drawings, looked for hazards inherent in the as-configured aircraft. They, not surprisingly, came up with two pages of safety concerns, which were subsequently closed out by corrective actions.

Documentation was used to control the safety program. The requirement that all safety efforts be documented provided a means of tracking all issues to their resolution. RSRA project management added an appendix to the AQP, as discussed earlier, which listed every request for action that resulted from major reviews, as well as concerns raised at informal reviews, staff meetings, or in casual conversations. Included in the listing was a notation of action taken, responsible person or organization, start date and completion date. A quick look at this report provided status in terms of issues identified, those resolved, and those remaining open.

5.2 IDENTIFYING VARIANCES. Progression through the phases of a development project results in variances from the original plan. While some of these variances are intentional, others are not. It is important to recognize them and assess their impact.

Waivers and deviations improperly handled can be the nemesis of any program. The problem becomes manifest when the pressure gets too great, and people tend to look for shortcuts. This situation may be evidenced by request for waivers, or qualification by similarity. This type of request should be noted as a possible danger signal. People tend to make "gut feel" trades between safety resources and/or schedule when the pressure is on. The RSRA probably accepted too many instances where the hardware was similar but the applications were not. A substantial workaround recovery mode was required at significant cost and schedule penalty to overcome the risks that resulted from accepting the similarity argument too easily. Waivers and deviations on the RSRA were handled by close coordination between contractor project engineers, the contractor's "third party" review (e.g., QC or Safety Committee), and the Government. Disposition of proposed waivers was handled at the project office level but with the advice and consent of third party reviewers. Such was the case when the need to waive the RSRA requirement for an operational EES prior to first flight was identified. This concern involved the ability of the crew to escape in the event of an emergency such as fire or mid-air collision. The escape system design and the allowable flight envelopes relative to desired aircraft performance bounds became "project drivers." The concern was identified early and pursued vigorously throughout the design, test, and operations; last-minute show stoppers were precluded. Through up-to-the-minute status and projections of escape system development, the project office was able to conclude that the qualification tests could not be completed prior to first flight. Armed with a current and detailed assessment of the impact on system safety/reliability of initial flights without an armed and qualified escape system, the project office was able to perform a credible cost/safety tradeoff in favor of cost, and to obtain concurrence by the Executive Safety Committee to waive the requirement for an operable escape system for initial flight. The RSRA risk management approach of early problem recognition and resolution provided a solution balanced among resources, performance, and safety.

5.2.1 Providing Flexibility. The practical view of the RSRA project management resulted in an AQP which provided flexibility. The plan was used as a daily working document, and progress was reported relative to it. Issues pertinent to the plan were discussed in regular staff meetings, and the plan was updated subsequent to its initial release in accordance with the preplanned schedule and to accommodate significant project changes, as shown in Figure 5.2-1.



NASA/ARMY

ROTOR SYSTEMS RESEARCH AIRCRAFT (RSRA)

AIRWORTHINESS QUALIFICATION PLAN

April 30, 1974

Revision	Date	Approval	Reason
A	June 19, 1974		Clarification
B	Nov. 22, 1974		Reschedule
C	April 21, 1975		Add Appendex (AQR)
D	June 7, 1976		Update CDR
E	Dec. 21, 1976		Update-Helo PFR and Reprogramming
F	Jan. 20, 1978		Update: Compound and AI/BS PFR

PREPARED BY: Samuel White, RSRA Project Office Chief Engineer

Robert K. Merrill, RSRA Project Pilot

APPROVED BY: Robert J. Huston, Manager, RSRA Project

CONCURRENCE: J. M. Patton, Jr., Langley Aviation Safety Officer

Figure 5.2-1 RSRA Airworthiness Qualification Plan Revision Page

There were a number of project events which precipitated changes in the physical plan itself, the areas of emphasis, or implementation of the plan. The impact of change is discussed in Section 6.0 of this document. It is briefly touched upon here to illustrate the need for flexibility in planning. Project changes can take many forms:

Personnel transfers. The project manager was replaced by the chief engineer, who subsequently filled both slots. Flexibility was inherent in the project staff. The project was already underway, the promotion came from within, and the chief engineer was exceptionally well qualified.

Project relocation. The RSRA project was relocated from Langley to Ames. Loss of corporate memory and changes in contractor support levels resulted. Special training and increased travel were imposed. Although these requirements were not anticipated in the planning, they were met through the adaptability of Government and contractor personnel.

Resource reduction. Resources allocated to the RSRA project were reduced, resulting in a need for descoping. Cost/performance/safety trades identified areas of least-hurt. This unplanned contingency resulted in reduction of safety activity in some areas and a schedule slip in at least one other case.

Schedule slips. PDR and CDR schedules were slipped as a result of project technical problems. The taxi-meter effect was minimized through the use of the incremental review concept. At least one safety issue arose, however, as a result of the unexpected delay which is discussed more fully in Section 6.0.

Each of these conditions was experienced at least once during RSRA development. The AQP provided the flexibility to accommodate these conditions in most cases. In others, the AQP itself was changed to meet project needs. The balance was made up by the adaptability of the project team. The need for built-in flexibility and adaptability is an important lesson learned which is directly applicable to future developmental aircraft projects.

5.2.2 Third Party Reviews. The scheduled project reviews served to identify variances, and safety-related activities external to the project often provided additional opportunities for assessment. During the RSRA project, two NASA-wide activities presented this type of target of opportunity. One such opportunity to identify variances by a third party was a board convened to audit safety practices on major NASA flight projects. The other, in September 1978, reviewed hardware failures in NASA projects to assess safety implications. This method of problem solving brought to bear resources not normally resident within the project. It enabled exploration of all avenues and allowed the manager to stay technically on top of his project. Another technique used consistently on the RSRA was the "top ten" approach as discussed in Section 3.1.4.

In response to the guidelines provided by the failure review panel, RSRA management identified a dozen failures/incidents that were "significant" by the panel's definition. An example was: "Failure of a piece of flight type hardware to operate properly and safely or to meet specifications relative to flight safety requirements which (based on available data) may adversely and significantly affect flight safety, program cost, or schedules or mission accomplishment." A summary of RSRA "significant" failures/incidents is provided in Figure 5.2-2.

FAILURE/INCIDENT ASSESSMENT PANEL REVIEW
Ames Research Center - November 8, 1978

PROPOSED RSRA AGENDA

Item	Failure Category	Failure/Incident	Avail. Data Indicates Effect On: Cost or Schedule	Safety	Mission
1	A(a)	Thermal relief plug in alighting gear wheels functioned, resulting in deflated tire	Yes*	No	Minor
2	A(b)	EES Blade Severance Assembly failed to function in environmental qualification tests, due to chemical breakdown of detonation charge at 200°F	Yes*	No	No
3	A(c)	Flight data indicated gross error in rotor load research measurement system	Yes*	No	Unknown
4	B	EES deployment bag contacted empennage/tail rotor area of aircraft at 209 kts, resulting in usable escape envelope less than operating envelope	Yes*	No	Yes
5	C	Emergency Escape System seat pendant cutter failed to function in environmental qualification tests, due to "blow by" around o-ring seal	Yes*	No	No
6	D	Stress corrosion crack discovered in TF34 auxiliary engine support fittings	Yes*	No	No
7	E	AIBS isolators in roll axis exhibited locked-out characteristics below 400 lbs vibratory force	Possible	No	Unknown
8	E	Dual wing tilt actuators did not work in harmony in the stalled system environment, resulting in differential loading of the wing	Yes*	No	Possible
9	F	Tail rotor ran out of directional control authority at 15 kts right sideward flight and fatigue loads exceed endurance limit in hover, due to greater than predicted T.R. blockage by vertical tail	No	No	Trival
10	F	Longitudinal stick margin at 153 KCAS, neutral cg was less than predicted, indicating potential controllability margin problem at aft cg	Minor	No	No
11	G	EES seat barostat functioned during installation, resulting in release of shoulder harness and seat buckle and initiation of chute deployment	Minor*	No	No
12	H	Ground operation of TF34 aux engines in crosswind without rotors turning caused tail rotor blade to impact flapping stops, damaging TR and requiring replacement	Yes*	No	No

* Cost impacted development program. Will not impact operational costs significantly.

Figure 5.2-2 Failure/Incident/Assessment Panel Agenda

This special review benefited the RSRA project in two ways: (1) Preparation for the review required the RSRA project office to review, categorize, and assess hardware failures that had occurred during the project; and (2) the review itself focused the combined judgment of the panel members on verification of satisfactory failure and recurrence control.

The importance of implementing recurrence control is exemplified by item 6 on the review agenda - stress corrosion cracking in TF34 auxiliary engine support fittings. Early in the design phase, it was established that 7075-T6 aluminum was not suitable for use in the aircraft structure. Rescheduling caused by other problems resulted in a delay in design of the auxiliary TF34 engine supports. By the time the design effort was resumed, the original airframe design team had been virtually disbanded and a new, smaller team staffed. The stress corrosion failure in the TF34 fittings was found to result from the use of 7075-T6 aluminum. This incident, and the other benefits derived on the RSRA project, demonstrate that this type of review should be included in future programs.

Issues, such as this, involving major program impact, were escalated to the level required to achieve resolution/approval. An example of this course of action involved the question of flying in the helicopter configuration without a qualified EES. As discussed earlier in the section, the issue, with supporting analyses, was carried forward to a "third party" Aviation Safety Committee and the Langley Executive Safety Board for confirmation (or redirection) of the recommendation to waive the requirement for an operational EES for initial helicopter flights. Approval was granted based upon special procedures and operational limitations.

While the RSRA was being developed, a systematic review method was being created at the Naval Postgraduate School under the direction of Mr. Charles Overbey. He produced a document which consisted of critical questions related to each major functional area. These questions stand in sharp contrast to the usual yes-no checklist questions and are typical of the type which have been, or should be, asked in design and operation evaluations. The technique established in his document was applied to the RSRA by the project manager as a target of opportunity. A sample page from the resulting report is shown in Figure 5.2-3.

At least five critical safety issues were identified and subsequently resolved through application of this technique. Use of this "what if" technique also served to develop the special safety-related skills and traits critical to overall project success. As a specific example one EES reviewer asked, "What if the rotor blade pyrotechnic separation system does not sever all five blades and the crewmembers are extracted through the rotating blade?" The initial answer seemed obvious -- an interconnect was required. A closer look, however, revealed that the complexity of an interconnect system actually <u>decreased</u> the probability of survival; but the value of asking key questions was established, and a more comprehensive analysis resulted.

PROJECT: Army/NASA RSRA OVERBEY REPORT 22

1.0 Emergency

1.1 Are full scale blade separation tests planned? Do these tests evaluate the effect of shrapnel?

1.2 Do the engineering analyses and test results give reasonable assurance that shrapnel from the rotor blade cutting action will not pose a threat to safety of the crew and will not pose a threat to integrity of vital aircraft systems?

1.3 Will the short rigid line attached to the blade severence assembly be thrown free and possibly strike a vital part of the aircraft?

1.4 Do planned test satisfactorily cover the expected aircraft airspeed range for initiation of blade severance?

1.5 Do these tests cover severed blade clearance of the tail of the aircraft?

1.6 Are there any conditions of uncontrolled flight (rolling, pitching yawing, inverted, etc.) where the jettisoned blades can strike the aircraft? If so, have they been evaluated to assure minimum risk for crew bail-out?

1.7 Has the blade separation rotary transfer unit, which was designed especially for this aircraft, been thoroughly qualified by analysis and test?

1.8 Are the pyrotechnic lines internal to the rotor drive shaft supported in a satisfactory manner?

1.9 The flexible lines which connect across the blade hinge are subject to constant flexing with each revolution of the rotor. They are also exposed to buffeting and vibration. Are these flexible lines of such material and size, and are they so supported, as to minimize adverse effects of constant flexing, vibration and buffeting?

1.10 What would be the expected effect of failure of one of these ten (10) flexible lines in normal operations? Would such failure create a serious hazard? If so, should these lines be periodically inspected and/or replaced on an empirical basis?

Figure 5.2-3 RSRA Overbey Report Example

5.3 IMPLEMENTING MODIFICATIONS. Failures and/or incidents occasionally necessitated hardware or programmatic changes. Decisions regarding those modifications were based on assessment of impact on cost, schedule, safety and the mission. A driver in every case was the need to maintain or improve the desired level of safety.

As discussed earlier, the FMEA's were used to provide subsystem and system hazard identification. This was not an ideal solution, but was the best that could be done under the circumstances, and it illustrates the type of tradeoffs that may be required to recover from unforeseen problems.

Another example of task realignment employed by RSRA management early in the project was to shift effort from less critical to more critical areas. One case involved fatigue substantiation. The original RSRA specifications required the performance of fatigue analysis; however, cost of the analysis exceeded the project budget. In the ensuing efforts by the Government to align the cost and budget, the specification for fatigue analysis was changed. The contractor's interpretation of the revised specification was to substantiate fatigue by static loads. This type of analysis is not very meaningful for helicopters, particularly for the RSRA which is subject to fatigue not just in the rotor system but also in the airframe, because of the unique configuration of the measurement systems. From a safety point of view, this situation was unacceptable, and the RSRA Chief Engineer shifted some assignments to obtain a gross fatigue analysis. Man-hours allotted for weight and balance tracking and for load analysis were traded to perform this effort. The effort expended on weight and balance tracking was held to an absolute minimum and the load analysis was performed largely by the Government rather than by the contractor.

Deletion of the fatigue analysis will probably plague the RSRA project for the operational life of the aircraft. Operations will be kept safe, but at the substantial price of delays to the flight research program.

Concern over delays to the program resulting from inadequate fatigue analyses manifested themselves early in research operation. The compound version of the RSRA has, in fact, been grounded for substantial periods because of unexpectedly high fatigue loads in the horizontal stabilizer.

5.4 DOCUMENTING HAZARDS. A closed-loop hazard tracking system was established in which status of all identified hazards was recorded and tracked. The RSRA program accomplished this by the addition of an appendix to the AQP called the AQR. The AQR provided a complete listing of all concerns identified during the RSRA project and the required resolution action. Figure 5.4-1 is an excerpt from the AQP which describes the format and content of the report.

Risks or concerns for airworthiness of the RSRA shall be identified, actions required to resolve these concerns shall be established and scheduled, and a summary of resolution actions required or taken shall be presented in this AQR. The summary listings shall be included in the agenda of major program reviews.

Table II provides a master listing of airworthiness concerns identified during the program, along with detailed actions required to resolve these concerns. The origin of the concern is also identified to provide a visible audit trail.

Table III presents a resorting of Table II actions by major program review milestones and provides airworthiness agenda items for each program review. Following each program review, any open items from Table III or any new actions generated from the review will be carried forward to future reviews in Table III. Table III agenda items from completed reviews will be deleted since they are retained in Table II.

In order to fully document and date specific actions taken to close out AQP items, Summary Lists I-XI will be used. The Summary Lists will also be used by the Project Office to continually track action status between major reviews. These lists are oriented on specific events throughout the program, to include Table III reviews, plus any other significant activity identified. Upon completion, they provide a comprehensive index of close-out documentation. They will be used as a final checklist to insure completion of required actions prior to the event specified and will become a permanent part of this AQR when completed.

Figure 5.4-1 Excerpt from the Airworthiness Qualification Report

Table II of the AQR provided a complete list of all concerns identified during the RSRA project. The table identified the subsystem to which the concern was related, a brief statement of the concern, the actions required to resolve the concern, the completion status of the actions, and a reference to how the concern was identified and reported. An example of a page from this table is presented in Figure 5.4-2.

..S	RISK OR CONCERN	RESOLUTION (OR ACTION REQUIRED)	REFERENCE
FLIGHT CONTROLS			
11E-8	Concern for structural integrity and mechanical reliability of control system and components (including jam modes of failure).	*1. Review design details at CDR.	RFA 7/11/74/VI-11
		*2. Review FMEA's prior to FRR.	7/11/74-VI-12
		*3. Review test plans (Qual. test, acceptance tests pre-flight ground tests) prior to tests, and review test results prior to FRR	7/11/74-VI-14 7/11/74-VI-16
		*4. Review configuration at first article inspection prior to FRR	RFA7/9/76-FRR-15 -12
		*5. Verify flight loads prior to envelope expansion.	
11E-9	Concern for ground crew safety with actuation of drag brake.	*1. Provide ground safe device; confirm at CDR (Removable pin)	RFA 7/11/74-VI-13
		...und test and first ...compound test.	
11E-10 (11B-5) (11J-1) (11L-5) (11N-1)	Concern for co... integratio... install... subs...		
11E-11			

Figure 5.4-2 Example of AQR Table II

Table III of the AQR listed the concerns that were not resolved prior to a project review and were agenda items for that review. Following each review, a new sheet was added to Table III to carry forward any open concerns for consideration at the next review.

The AQR also included summary tables of concerns requiring action prior to specific project milestones. These tables contained basically the same information as shown in Table II, but they also contained a reference to the resolution documentation for the concern and the date the resolution was effected. An example summary page is presented in Figure 5.4-3.

SUMMARY - ACTION ITEMS

Revised July 12, 1977
Final revision

I. Completion Required Prior to Resumption of Helo Flights (Flights resumed 7/13/77)

ITEM NO.	RISK OR CONCERN	RESOLUTION OR ACTION REQUIRED	REFERENCE	CLOSEOUT REFERENCE	DATE
I-1	EMI	Perform/verify EMI tests	SOFR 9/29/76 AQPIII-11E-6	Langley memo to Merrill 7/7/77, 256/R. Murray	7/7/77
I-2	Fuel System	Perform/verify fuel system calibration and ATP	SOFR 9/29/76	RSRA Memo to Files, 246E/SWhite:bpj	6/23/76
I-3	EFCS	Perform/verify EFCS ground tests	SOFR 9/29/76	Langley Memo to Merrill 7/7/77, 256/R. Murray	7/7/77
I-4	Proof operational ...	Perform/verify/proof/...	SOFR 9/29/76	Sikorsky ETR per J. Brilla	7/12...

Figure 5.4-3 Example of AQR Summary Table

The technique employed by the RSRA project for documenting hazard resolution was excellent. It provided for a complete listing of all identified hazards and a record of the resolution action implemented. Thus, any hazard or concern could be traced from identification through verification of resolution.

The RSRA experience has demonstrated some basic truths related to hazard documentation which can be applied to future projects. A record should be maintained of all concerns and not just those considered significant. Resolution action should be verified before the issue is closed. This leaves a clear audit trail. Years later it may become necessary to reconstruct the actions taken and rationale for decisions made. Finally, allowance should be made for updating the documentation as warranted by additional knowledge and time. This flexibility is essential in maintaining a viable document consistent with realistic needs of developmental projects.

6.0 ADAPTING. A host of ills can beset the manager after the project is well underway and (he thought) under control. Programmatic changes beyond control of the manager can be devastating. If not properly handled, chaos will result. Potentially disruptive changes occurred on the RSRA project with some regularity, but built-in adaptability ensured positive project direction and control.

The AQP established milestones for completion of each program phase. However, some events beyond management control resulted in schedule slippage, but not in loss of project control. Flexibility was the key. The ability to adjust schedules because of safety considerations and without further compromising safety was essential. The night before the PDR, an aerodynamic instability problem was revealed by wind tunnel testing. The resolution of the problem required redesign of the tail. Obviously, that section of the aircraft was not ready for even preliminary design review. It was decided, however, to proceed with the design review of the aircraft, with the exception of the tail and the auxiliary engine mounts which would probably change to offset the center of gravity shifts which would result from tail redesign. A delta PDR was held after redesign of the tail to ensure that system safety and performance had not been compromised. The decision resulted in a 6-month project slip to ensure safety. As a part of the delta PDR, results of the previous segments of the review were re-evaluated to ensure their currency and continued validity. That's an important thing to remember for future projects.

The next major system review, the system CDR, was originally scheduled to follow the last of the subsystem CDR's. It was decided, however, because of schedule slippage, to conduct the system CDR prior to completion of the EFCS, AI/BS, and EES subsystem CDR's. Workaround plans were prepared to accommodate installation of the affected systems after first flight of the helicopter to minimize the impact on overall project schedules. The resulting schedule for the CDR's is shown in Figure 6.0-1 below.

WBS	SYSTEM	CDR DATE
11A	AIR FRAME	JUNE 10, 1975 (final)
11B	SECONDARY POWER	JANUARY 8,1976
11C	PRIMARY POWER	MAY 7, 1975
11D	LIFE SUPPORT/ENVIRONMENTAL	MAY 7, 1975
11E	FLIGHT CONTROLS	JANUARY 8, 1976
11F	DRIVE	FEBRUARY 6, 1975
11G	ROTOR	FEBRUARY 6, 1975
11H	ENGINES	MAY 7, 1975
11J	AVIONICS	FEBRUARY 6, 1975
11K	EMERGENCY ESCAPE	FEBRUARY 6, 1976
	- STATUS REVIEWS	JUNE 10 AND NOV. 11, 1975 JAN. 30 AND FEB. 11, 1976
	- FINAL CDR (HOLLOMAN TEST READINESS)	AUGUST 6, 1976
	- POST HOLLOMAN TEST REVIEW	APRIL 14, 1977
	- QUALIFICATION REVIEW	JUNE 16, 1977
11L	ONBOARD RESEARCH INSTRUMENTATION	MAY 7, 1977
11M	ACTIVE ISOLATOR/BALANCE SYSTEM	
	- STATUS REVIEW	JANUARY 22, 1975
	- FINAL CDR	JULY 1, 1976
11	SYSTEM (RECONFIRMED AFTER 11E)	JULY 1, 1976

Figure 6.0-1 RSRA Incremented CDR Schedule

As shown by this example, the plan evolved with the project. This flexible approach enabled project management to stay abreast of the changing nature of hazards as the design, development, and test phases of the project were accomplished.

Again, as with the PDR, it was necessary to re-evaluate total system posture after completion of the delta reviews. Stress corrosion cracking of the engine support fittings, described in Section 5.2.2, resulted from use of a prohibited material, which was a configuration control problem. Slack time during the CDR slippage probably fostered some laxity which allowed the problem to happen. That was a review discipline problem.

Ten months after initiation of RSRA flight tests at the contractor's plant, the flight test operations were transferred to NASA-Wallops Flight Center (WFC) with the intent of phasing over from contractor to Government flight operations by Langley at WFC. In mid-stream, NASA transferred the helicopter roles and missions from Langley to Ames. As a result, a year and a half after starting operations at WFC, one of the two aircraft had to be transferred to Ames Research Center for continuation of its flight testing. One year after that, the other aircraft was also transferred to Ames for completion of development flight testing and for research flight operations.

During the first of these site relocations, there was a transition from operations at the contractor plant (fully supported not only by the project team, but by the aggregate of all of the contractor's support personnel and facilities) to remote site operations by a small contractor team supported by a different Government-operated flight facility. During the transfer from WFC to Ames, in addition to the change in flight facility, there was a transition from operation by a contractor team monitored by a Government team, to operation by the Government team supported by a contractor team. These difficulties were compounded by lack of travel funds to permit continuity of Government team participation, as well as by periodic rotation of contractor personnel from the remote site back "home."

These changes in site and transition between contractor and Government teams resulted in a partial loss of corporate memory. This loss was compounded by a decision early in the program to adopt the experimental shop approach to documentation for reasons of cost. A complete set of preliminary drawings and changes (but not final drawings) was eventually forwarded to Ames. The results of these changes and early decisions have not degraded the safety of the RSRA, but have made the maintenance of the desired degree of safety more difficult.

Transition from the project development phase to the operational phase is normal, but it is not without its own special problems. Probably the single most difficult problem deals with corporate memory loss as discussed above. The problem is compounded on R&D, one-of-a-kind projects, because traditional "fleet" documentation is usually not prepared. New people are unfamiliar with development problems, and there are no established training programs.

Key operations-type personnel (just like safety) should be integrated into the development project early. Such an interlocking arrangement will minimize transition problems and enable an on-schedule release for flight as shown in Figure 6.0-2.

A-35

1976

National Aeronautics and Space Administration

Langley Research Center
Hampton Virginia
23665

NASA

SEP 29 1976

246E

Sikorsky Aircraft Division
United Technologies Corporation
Attn: Mr. Merrick W. Hellyar
Stratford, CT 06602

Subject: Safety-of-Flight Release, Contract NAS1-13000, RSRA

Based on the results of the final safety-of-flight review at the September 28, 1976 Pre-Flight Review, authorization is granted for release of the RSRA for flight tests, with the following conditions and limitations:

1. Configuration. - This Safety-of-Flight release applies ... the RSRA helicopter configuration ... Escape System ... all downing (red x) discrepancies for aircraft ... NASA 546.

This Safety-of-Flight release is further conditional upon satisfactory completion and resolution of the following open items from the Pre-Flight Review of September 23, 1976:

1. Prior to flight with SAS 1 and 2 actuators:

   a. Substantiate structural integrity for vibration/fatigue and revalidate qualification status.

   b. Measure SAS actuator motion to verify summing and verify acceptability of hardovers.

   c. Verify collective ... settings.

2. Prior ... EMI safety checks.

5. Prior to installation of load limiter shear pin, verify integrity for limit load.

6. Prior to performance to monthly periodic inspection (due October 31, 1976) verify EFCS monthly inspection procedure, ETP 72T2-00004.

Donald P. Hearth
Director

Figure 6.0-2 Conscientious Application of Safety Principles by Dedicated and Technically Superior Project Teams Leads to Release for Flight

CONCLUDING REMARKS

This document has provided insight into establishing and implementing a safety program for developmental aircraft projects. It has demonstrated, through examples, the approach taken by the RSRA project management. Though not always in accordance with the classical approach to system safety, this method was effective and successful. This success is a direct result of planning, organizing, directing, and controlling the project with the proper degree of emphasis on safety.

A specific conclusion to this document, covering more than 6 years of RSRA history, is perhaps best supplied by the former RSRA Project Manager/Chief Engineer, Sam White:

- Apply the basic principles of management, especially those that fall into the category of safety tasks. The safety tasks are finite and do-able and, properly done, they'll reduce risks.

- Plan the safety activities (who, what, when). Use whatever specs, standards, or regulations you want, but use an authoritative requirements document and tailor it to fit the project.

- Not only plan the work, but also work the plan. Track it with fairly rigorous discipline and document the audit trail, paying attention to details. This takes work, but it not only prevents dropping something down the crack and provides "CYA" paper, it also creates an attitude and awareness that safety is real and really beneficial to the project, not just a burden.

- Assign a competent chief engineer who is clearly accountable not only for safety but also for mission/system performance. Permit (encourage!) him to take an adversary role viz the Project Manager on cost/schedule versus safety tradeoffs. Don't delegate the tough problems.

- Use the jury concept in project reviews and in making conscious decisions to accept risks. Make sure "calculated risks" are truly <u>calculated</u>.

- Use the top ten approach. Start with the ten highest technical risk areas and list all actions to be taken to resolve them. As real problems emerge, establish top ten problem actions. Go down alternative or contingency paths <u>in parallel</u> with best solution path; don't wait to do it <u>in series with a</u> "no go" on the best path. In other words, <u>tend to</u> overkill top ten problems.

- If you are faced with a resource-impacting event -- such as a funding cut -- you will want to consider waivers, qualification by similarity, descoping, reassignment of duties, and possibly an "experimental shop" approach. Any of these methods can be employed with success. However, the experimental shop approach is not recommended due to the loss of controllability. If you choose to waive requirements, be sure to make deliberate, informed decisions -- not default decisions. Likewise, in using shortcuts -- such as qualification by similarity -- verify that similarity really exists in all pertinent areas: Environment, use, life cycle, etc. The point is, consider the safety aspects in making your management decisions.

- Communicate problems to "management." Present options and your recommendations ("cancel the program" is an option that needs to be addressed, even if you don't recommend it). Do this early enough, when the options still exist; don't delay to the point of forcing the default option.

In addition to Mr. White's synopsis of RSRA experience, a more generalized conclusion in retrospect is provided. The approach taken by RSRA management in planning the safety program was to integrate the safety goals into the project goals. This approach was initiated by incorporating safety requirements into the AQP. This deviated from the more standard approach of providng a separate safety plan by providing a single document for project guidance with emphasis on safety as well as performance. The ultimate use of the aircraft to be developed was considered in the definition of all program requirements.

Requirements tailored to the specific needs of the RSRA project carried through the organizations of the work as well. "Horse-trading" of resources was performed to apply project emphasis in the most critical of areas. Actions such as these trades, effected by project management, are definitely a deviation from the more standard approach which tends to satisfy contract requirements regardless of project need. Contract requirements were satisfied on the RSRA project, but through these "horse-trades" the emphasis of the project was shifted, when necessary, toward safety. Another deviation from the more conventional organization was the lack of a separate safety staff. The RSRA project management established a safety focal point supported by the subsystem managers. This emphasized safety as an integral part of project success and required that the most knowledgeable and competent personnel be involved in the safety effort. Even the test pilots were involved throughout DDT&E and were integrated into the project "family" to promote safety consciousness and inject human factor considerations into the design.

The RSRA attitude toward safety was also significantly influenced by the project manager's personal characteristics. His safety-conscious approach to project direction was demonstrated by such things as seminars conducted to educate the staff in safety principles. Education of staff members is not always included in the approach to system safety, but definite benefits were evidenced in the RSRA project.

CONCLUDING REMARKS

Just as the plan and organization were adapted to the specifics of the RSRA project, the safety tools which were applied in the project were selected to provide maximum return for resources expended. The decision to apply or omit the application of particular safety tools was carefully weighed. In some cases, additional tests and procedures were substituted for certain analyses. In the long term, these substitutions were not always cost effective. For example, application of sneak circuit analysis earlier in the project could well have circumvented the need for some extra tests and special procedures. Likewise, the performance of a PHA earlier in the project than actually performed would have provided more useable results. On the other hand, the redirection of the FMEA toward assessing criticality rather than probability of failures was an excellent example of good safety management.

The application of the safety tools identified safety concerns, as did the subsystem and system reviews. The decision to include knowledgeable people who were not involved with the project on the review boards was a profitable deviation from the normal methods for controlling a project. The perspective and insight provided by these third party experts added significantly to the safety value of the meetings. Another example of excellent management was seen in applying the Overbey technique to the RSRA. There was no requirement for the applications of the technique, and some additional effort was required of the project staff. This extra effort identified concerns at a point in the project which permitted resolution before serious problems arose.

An innovation by the RSRA project management, the AQR, greatly benefited the RSRA project by providing complete documentation of safety concerns. This prevented duplication of effort while ensuring that all concerns were resolved. In a like manner, the use of the top ten problems concept assured that concerns were elevated to the proper levels of management and focused the proper attention to the more critical issues.

Finally, history has shown that the approach of the RSRA project management provided adequately for safety. The approach alone did not accomplish this, but the commitment of an astute project manager, supported by a dedicated staff, resulted in a safe and successful project. Project safety can, therefore, be seen as achievable by maintaining a safety-conscious environment coupled with a systematic approach to balancing performance, resources, and safety at all times. RSRA stands as a witness to the efficacy of these techniques for safety.

REFERENCES

REFERENCES

AFSC Design Handbook DH1-3, Human Factors.

AFSC Design Handbook DH1-6, System Safety.

Brown, David B.: Systems Analysis and Design for Safety. Prentice-Hall, Inc., 1976.

Hammer, Willie: Handbook of System and Product Safety. Prentice-Hall, Inc., 1972.

Johnson, W. G.: The Management Oversight and Risk Tree. U.S. Government Printing Office, 1973.

National Aeronautics and Space Administration: NASA Safety Manual, Volume 1, Basic Safety Requirements. NHB 1700.1(V1), 1969.

National Aeronautics and Space Administration: NASA Safety Manual, Volume 3, System Safety. NHB 1700.1(V3), 1970.

1. Report No. NASA CR-3534	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle A System Safety Model for Developmental Aircraft Programs		5. Report Date April 1982
		6. Performing Organization Code
7. Author(s) Emil J. Amberboy and Robert L. Stokeld		8. Performing Organization Report No.
		10. Work Unit No.
9. Performing Organization Name and Address Boeing Aerospace Company Houston, Texas		11. Contract or Grant No. NAS2-10361
		13. Type of Report and Period Covered Contractor Report
12. Sponsoring Agency Name and Address National Aeronautics & Space Administration Washington, D. C. 20546		14. Sponsoring Agency Code RTOP 532-03-11
15. Supplementary Notes Ames Technical Monitor: Richard N. Young Final Report		

16. Abstract

This document presents some basic tenets as applied to developmental aircraft programs. It does not discuss the philosophy of system safety nor does it present instructions for applying system safety principles to a project. Rather, the integration of safety into the project management aspects of planning, organizing, directing, and controlling is illustrated by examples. The examples presented here are taken from the joint NASA/Army Rotor System Research Aircraft (RSRA) Project. The basis for project management use of safety and the relationship of these management functions to "real-world" situations encountered on the RSRA Project are presented. In each example both the rationale which led to the safety-related project decision and the lessons learned as they may apply to future projects are presented.

17. Key Words (Suggested by Author(s)) Aircraft, Development, Safety, Model, Airworthiness	18. Distribution Statement UNCLASSIFIED - UNLIMITED STAR CATEGORY - 03

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price*
UNCLASSIFIED	UNCLASSIFIED	81	A05

*For sale by the National Technical Information Service, Springfield, Virginia 22161

NASA-Langley, 1982